NetScaler 9000 Series

Installation and Configuration Guide - Vol. 1

180 Baytech Drive
San Jose, CA 95134
Phone: 408-678-1600, Fax: 408-678-1601
www.netscaler.com

NetScaler Part No.: NSICG60vol1 **Printed: January 2005**

© NETSCALER, INC., 2005. ALL RIGHTS RESERVED. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS OR USED TO MAKE DERIVATIVE WORK (SUCH AS TRANSLATION, TRANSFORMATION, OR ADAPTATION) WITHOUT THE EXPRESS WRITTEN PERMISSION OF NETSCALER, INC.

ALTHOUGH THE MATERIAL PRESENTED IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE ALL RESPONSIBILITY FOR THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS MANUAL.

NETSCALER, INC. OR ITS SUPPLIERS DO NOT ASSUME ANY LIABILITY THAT MAY OCCUR DUE TO THE USE OR APPLICATION OF THE PRODUCT(S) DESCRIBED IN THIS DOCUMENT. INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. COMPANIES, NAMES, AND DATA USED IN EXAMPLES ARE FICTITIOUS UNLESS OTHERWISE NOTED.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without NetScaler's written authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the NetScaler Request Switch™ 9000 Series equipment. If the NetScaler equipment causes interference, try to correct the interference by using one or more of the following measures:

•Move the NetScaler equipment to one side or the other of your equipment.

•Move the NetScaler equipment farther away from your equipment.

•Plug the NetScaler equipment into an outlet on a different circuit from your equipment. (Make sure the NetScaler equipment and your equipment are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by NetScaler, Inc., could void the FCC approval and negate your authority to operate the product.

BroadCom is a registered trademark of BroadCom Corporation. Fast Ramp, NetScaler, and NetScaler Request Switch are trademarks of NetScaler, Inc. Linux is a registered trademark of Linus Torvalds. Internet Explorer, Microsoft, PowerPoint, Windows and Windows product names such as Windows NT are trademarks or registered trademarks of the Microsoft Corporation. NetScape is a registered trademark of Netscape Communications Corporation. Red Hat is a trademark of Red Hat, Inc. Sun and Sun Microsystems are registered trademarks of Sun Microsystems, Inc. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright 1998 © Carnegie Mellon University. All rights reserved. Copyright © David L. Mills 1993, 1994. Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Copyright © Jean-loup Gailly and Mark Adler. Copyright © 1999, 2000 by Jef Poskanzer. All rights reserved. Copyright © Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves. All rights reserved. Copyright © 1982, 1985, 1986, 1988-1991, 1993 Regents of the University of California. All rights reserved. Copyright © 1995 Tatu Ylonen, Espoo, Finland. All rights reserved. Copyright © UNIX System Laboratories, Inc. Copyright © 2001 Mark R V Murray. Copyright 1995-1998 © Eric Young. Copyright © 1995,1996,1997,1998. Lars Fenneberg. Copyright © 1992. Livingston Enterprises, Inc. Copyright © 1992, 1993, 1994, 1995. The Regents of the University of Michigan and Merit Network, Inc. Copyright © 1991-2, RSA Data Security, Inc. Created 1991. Copyright © 1998 Juniper Networks, Inc. All rights reserved. Copyright © 2001, 2002 Networks Associates Technology, Inc. All rights reserved. Copyright (c) 2002 Networks Associates Technology, Inc. Copyright 1999-2001© The Open LDAP Foundation. All Rights Reserved. Copyright © 1999 Andrzej Bialecki. All rights reserved. Copyright © 2000 The Apache Software Foundation. All rights reserved. Copyright (C) 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved.

Contents

Chapter- 1
Introduction to the NetScaler 9000 Series 1-1
1.1 - Who Should Use This Book 1-1
1.2 - How to Use The NetScaler 9000 Series Guides 1-2
1.3 - Documentation Conventions 1-5
1.4 - The NetScaler 9000 Series 1-5
1.5 - Features at a Glance 1-10
1.6 - Technical Support and Resources 1-17

Chapter- 2
Installation, Configuration and Management 2-1
2.1 - System Models 2-1
2.2 - LCD Monitor in NetScaler 9000 System 2-4
2.4 - Configuring the NetScaler 9000 System 2-25
2.5 - Maintaining the NetScaler 9000 System 2-43
2.6 - Managing the NetScaler 9000 System 2-44
2.7 - Path MTU Discovery 2-78
2.8 - Understanding NetScaler License Keys 2-81
2.9 - Autodetect Service 2-84

Chapter- 3
High Availability 3-1
3.1 - Overview 3-1
3.2 - Considerations for High Availability Setup 3-3
3.3 - Configuring two NetScaler 9000 systems in High Availability Mode . . 3-6
3.4 - Changing to a High Availability Configuration 3-10
3.5 - Verifying Configuration Propagation 3-13
3.6 - Forced Synchronization 3-14
3.7 - Force Failover of the Primary NetScaler 9000 System 3-15
3.8 - Forcing the Secondary Device to Stay Secondary 3-17
3.9 - Troubleshooting HA Issues 3-18

Chapter- 4
NetScaler Statistical Utility 4-1
4.1 - Overview 4-1
4.2 - Accessing NetScaler Dashboard 4-2
4.3 - Understanding Graphs and Legends 4-6
4.4 - Dashboard Components 4-7
4.5 - Monitoring Performance Statistics of Key NetScaler Features 4-17

Appendix- A
Policy Expressions A-1
A.1 - Understanding Expressions A-2
A.1 - Using an expression in a policy definition A-14

Appendix- B
NetScaler API Reference B-1
B.1 - Introducing NetScaler Application Programming Interface B-1
B.2 - Benefits of NetScaler API B-2
B.3 - Hardware and Software Requirements B-2
B.4 - Interface Description B-2
B.5 - NetScaler API Architecture B-3
B.6 - The NSConfig Interface B-4
B.7 - Example: Setting the NetScaler Configuration B-5
B.8 - Example: Querying the NetScaler Configuration B-6
B.9 - The Web Service Definition Language (WSDL) B-8
B.10 - Creating Client Applications using the NSConfig.wsdl File B-9
B.11 - Securing NetScaler API Access B-11

Appendix- C
Warning and Safety Messages C-1

Chapter 1
Introduction to the NetScaler 9000 Series

Welcome to the NetScaler 9000 Series Installation and Configuration Guide. This guide describes how to install, configure and manage all of the products included in the NetScaler 9000 product line and includes several sample configurations to assist you in planning for system deployment in your own network environment.

Topics included in this chapter are:

- Who Should Use This Book
- How to Use The NetScaler 9000 Series Guides
- Documentation Conventions
- The NetScaler 9000 Series
- Features at a Glance
- Technical Support and Resources

Note:

1. By default, this guide refers to the product as the *NetScaler 9000 system*.
2. When referring to the Secure Application Accelerator this guide uses specific model numbers: *9050, 9100, or 9500.*
3. When referring to the Secure Application Gateway, this guide uses specific model numbers: *9200, 9600* or *9900*.
4. When referring to the Secure Application Switch this guide uses specific model numbers: *9400, 9800* or *9950*.

1.1 Who Should Use This Book

The Installation and Configuration Guide is intended for developers, test engineers, system administrators or others who install and configure NetScaler 9000 systems into their network infrastructures.

Knowledge of the software and services running on web servers is needed to configure the system appropriately. Basic knowledge of networking and web technologies is assumed.

1.2 How to Use The NetScaler 9000 Series Guides

To help you use the NetScaler 9000 system and it's various features, this documentation set is contained in two volumes. These volumes are organized as follows.

1.2.1 Volume 1

This Volume covers the general use and management features of the NetScaler 9000 Series system. Refer to this guide for instruction on installation, management, administration, and all non-feature specific tasks.

- **Chapter 1, Introduction to the NetScaler 9000 Series**: This chapter describes the basic features and benefits of the NetScaler 9000 system. It also provides a brief description of the key features that can be configured on the NetScaler 9000 system.
- **Chapter 2**, **Installation, Configuration and Management**: This chapter describes how to install, configure and manage the NetScaler 9000 system.
- **Chapter 3, High Availability**: This chapter describes how to install and configure the NetScaler 9000 system in the High Availability mode.
- **Chapter 4, NetScaler Statistical Utility:** This chapter introduces you to the NetScaler Statistical Utility (also referred as the NetScaler Dashboard). It explains the various components of this graphical utility and also the steps to monitor the NetScaler 9000 system's performance using the Dashboard utility.
- **Appendix A, Policy Expressions:** This appendix provides an overview on constructing NetScaler Policy Expressions.
- **Appendix B, NetScaler API Reference:** This chapter provides information on the NetScaler Application Programming Interface (API) and detailed instructions on how to use this XML API to implement customized client applications.
- **Appendix C, Warning and Safety Messages**: This appendix provides various warning messages and their description.

1.2.2 Volume 2

In this Volume, you will find the documentation for the specific features available on the NetScaler 9000 Series system.

- **Chapter 1, Load Balancing**: This chapter describes the steps to configure and manage various Load Balancing (LB) feature in the NetScaler 9000 system.
- **Chapter 2, Firewall Load Balancing:** This chapter describes the steps to configure and manage the the Firewall Load Balancing feature in the NetScaler 9000 system.
- **Chapter 3, Global Server Load Balancing:** This chapter describes the steps to configure and manage the GSLB feature in the NetScaler 9000 system.
- **Chapter 4, Content Switching**: This chapter describes the steps to configure and manage the Content Switching (CS) feature in the NetScaler 9000 system.
- **Chapter 5, Cache Redirection**: This chapter describes the steps to configure and manage the Cache Redirection (CRD) feature in the NetScaler 9000 system.
- **Chapter 6, Configuring Integrated Caching:** This chapter describes the steps to configure and manage the Integrated Cache feature.
- **Chapter 7, Secure Sockets Layer (SSL) Acceleration**: This chapter describes the steps to configure and manage the Secure Sockets Layer (SSL) Acceleration feature in the NetScaler 9000 system.
- **Chapter 8, Secure Virtual Private Network (SSL VPN):** This chapter describes the steps to configure and manage the SSL VPN feature.
- **Chapter 9, Web Server Logging**: This chapter describes the steps to configure and manage the Web Server Logging feature in the NetScaler 9000 system.
- **Chapter 10, Performance**: This chapter describes the steps to configure and tune the various performance features in the NetScaler 9000 system, such as *Compression, Connection Keep-alive/server off load, Client Keep Alive and TCP buffering*.
- **Chapter 11, Protection**: This chapter describes the steps to configure and manage the various protection features in the NetScaler 9000 system, such as, *Surge Protection, Priority Queuing, DoS Protection, Content Filtering* and *protection from SYN attacks*

- **Chapter 12, Sure Connect**: This chapter describes the steps to configure and manage the SureConnect feature in the NetScaler 9000 system.
- **Chapter 13, Advanced Network Configurations**: This chapter describes how to configure advanced features such as, *Layer 2 Mode, Use Source IP addresses (USIP), MAC-based Forwarding* and *VLANs support* in the NetScaler 9000 system.
- **Appendix A, Optimizing Web Servers**: This appendix provides the steps to optimize performance for various web servers.
- **Appendix B, Converting Certificates and Keys**: This appendix provides steps to convert certificate and key format using the OpenSSL tool.
- **Appendix C, Fine Tuning Built-in Integrated Cache Behavior:** This appendix provides information on how to fine tune the built-in cachability behavior.
- **Appendix D, Built-in Behavior of Integrated Cache:** This appendix provides cache policies and the corresponding built-in cachability behavior.

1.3 Documentation Conventions

CONVENTION	ALERTS YOU TO:
`Command`	This typeface represents a command that you must type using the exact upper/lower case characters shown. After every command typed into the NetScaler 9000 Command Line Interface (CLI) press the **Return** or **Enter** key on your keyboard.
`Command argument`	This typeface represents a command argument.
`Screen text`	Text with this typeface represents information on a screen, as well as the names of directories, files and commands.
<Key name>+<Key name>	Keyboard key names appear within angle brackets. A plus sign appears between keys that you must press simultaneously.
Text in italics	Italic type emphasizes text or indicates new terms.
Initial Capital Letters	Names of windows, dialogs, tabs, menus, icons, buttons and other user interface elements start with capital letters.

ICON	NOTICE TYPE	ALERTS YOU TO:
NOTE	Information note	Important additional information
CAUTION	Caution	Risk of personal injury, system damage or data loss
WARNING!	Warning	Risk of severe personal injury

1.4 The NetScaler 9000 Series

The NetScaler 9000 Series of secure application networking systems is designed to protect and optimize the delivery of applications over the Internet and private networks. To achieve this, it combines application-level security, optimization and switching into a single, integrated solution. The NetScaler

9000 Series is comprised of three products: the Secure Application Accelerator (9050/9100/9500), the Secure Application Gateway (9200/9600/9900) and the Secure Application Switch (9400/9800/9950).

Each of these solutions is available in Fast Ethernet and gigabit configurations and can be integrated into any environment as a complement to existing load balancers, servers, caches and firewalls. The system requires no additional client or server side software and is easily deployed via the system's web-based GUI and CLI configuration utilities.

Refer to Secure Application Accelerator, Secure Application Gateway and Secure Application Switch in this chapter for a summary of various product models and their key features.

Note: The Secure Application Gateway and Secure Application Switch are also available for non-SSL environments. These products are denoted with a "-N" appended to the model number.

As a complement to the application networking features included in each of the products of the NetScaler 9000 Series, each system can be easily upgraded to support the following additional product options: Proximity-based GSLB and Application Caching.

1.4.1 Secure Application Accelerator - Models 9050, 9100 and 9500

The NetScaler Secure Application Accelerator is an entry-level solution that integrates secure remote access with application protection and optimization into a unified platform for secure application delivery. The Secure Application Accelerator can be deployed to enable client-less secure remote access via SSL VPN technology, and can serve as a security and optimization appliance to encrypt, protect and accelerate application delivery.

Table 1-1 Secure Application Accelerator product line.

Model Number	Network Interface	Key Packaged Features
9050 / 9100	2 10/100 Base-T Ethernet ports	Application Security • L2-4 DoS Protection • SSL VPN (1 concurrent user session) Application Optimization • TCP Offload • SSL Offload • Compression
9500	4 10/100/1000 BaseT or 4 Gigabit SX ports 1 10/100/1000 Base-T management port	

1.4.2 Secure Application Gateway - Models 9200, 9600 and 9900

NetScaler's Secure Application Gateway applies NetScaler's patented Request Switching™ technology to provide robust web application security, protection and optimization. The system is typically deployed as a complement to existing network architectures and can be used to instantly encrypt application data, continuously serve users, and reduce the total cost of operations, all without diminishing the user experience.

Table 1-2 Secure Application Gateway product line:

Model Number	Network Interface	Key Packaged Features
9200	2 10/100 Base-T Ethernet ports	Application Security • L2-7 DoS Protection • Content Filtering • Surge Protection • Priority Queuing • SureConnect™ • Consolidated Web Logging • SSL VPN (5 concurrent user sessions) Application Optimization • TCP Offload and optimization • SSL Offload • Compression
9600	4 10/100/1000 Base-T or 4 Gigabit SX ports 1 10/100/1000 Base-T management port	
9900	4 10/100/1000 Base-T or 4 Gigabit SX ports 1 10/100/1000 Base-T Mgmt. port	

1.4.3 Secure Application Switch - Models 9400, 9800 and 9950

NetScaler's Secure Application Switch augments the functionality of its Secure Application Gateway to provide fine-grain traffic management - uniquely combining application-level security, optimization, and layer 4-7 switching into a uniform platform. The system is typically deployed as a fully integrated traffic management system, in-line with traffic, to enable enterprises, e-businesses and service providers to ensure the cost effective, continuous, secure delivery of their business critical applications.

Table 1-3 Secure Application Switch product line

Model Number	Network Interface	Key Packaged Features
9400	2 10/100 Base-T Ethernet ports	Application Security • L2-7 DoS Protection • Content Filtering • Surge Protection • Priority Queuing • SureConnect™ • SSL VPN (5 concurrent user sessions) • Consolidated Web Logging Application Optimization • TCP Off load and Optimization • SSL Off load • Compression Application Switching • Load Balancing • Content Switching • Cache Redirection • Link Load Balancing • Global Server Load Balancing
9800	4 10/100/1000 Base-T or 4 Gigabit SX ports 1 10/100/1000 Base-T management port	
9950	4 10/100/1000 Base-T or 4 Gigabit SX ports 1 10/100/1000 Base-T Mgmt. port	

1.4.4 Proximity-based GSLB

With this license enabled, the NetScaler system can be configured to make its GSLB decision based on the proximity of the client browser's local DNS server (LDNS) to the destination site. Proximity can be determined dynamically (i.e. based on the current network status) or statically (based on the geographic location of the client and the sites, as defined on the system).

1.4.5 Application Caching Option

The Application Caching Option for the NetScaler 9000 Series enables enterprises and content providers to further improve their application

performance through the integration of in-memory static and dynamic caching.

1.4.6 Secure Remote Access User Packs

For those businesses that wish to increase the capacity of the Secure Remote Access (SSL VPN) feature in the NetScaler 9000 Series, additional user packs are available as a means of boosting the number of concurrent user sessions supported. By default, the Secure Application Accelerator supports one concurrent user while both the Secure Application Gateway and the Secure Application Switch support five concurrent user sessions, at no additional charges.

1.5 Features at a Glance

1.5.1 Application Intelligent Architecture

Based on NetScaler's Request Switching™ technology, the NetScaler 9000 system improves the throughput and scalability of application infrastructure by de-coupling the flow of application requests and responses from the underlying transport -- offloading transport processing from servers and freeing valuable CPU cycles. The NetScaler 9000 system then makes optimal use of transport protocols and resources – regulating the flow of requests, keeping long-lived TCP connections and multiplexing application level requests across them – maximizing efficiency even when all of the content is compressed or secured. By leveraging this unique ability to analyze requests and responses, the NetScaler 9000 system can identify and defeat Denial of Service attacks and intrusion attempts, recognize legitimate traffic and boost it in priority to ensure optimal end-user response times.

Request Switching includes the following traffic management techniques:

- Offloads transport processing from servers and caches
- Analyzes and optimizes every server response
- Provides adaptive regulation of request flow without transaction loss
- Keeps client TCP connections alive to speed response times
- Multiplexes and de-multiplexes application level requests to maximize server efficiency

1.5.2 Application Security Features

The Product Name (short) system includes the following traffic security features:

- SSL Off load and Acceleration
- Secure Remote Access (via SSL VPN)
- Distributed Denial of Service Attack (DDoS) Defense
- Content Filtering
- Surge Protection
- Priority Queuing
- SureConnect™

1.5.2.1 SSL Off Load and Acceleration

SSL can place a heavy burden on an application's performance and because of encryption, can render many optimization measures ineffective. NetScaler has incorporated high performance SSL acceleration as a core part of its solution, transparently offloading the CPU-intensive SSL encryption/ decryption from local web servers and freeing server resources to service other content requests. All of the benefits of NetScaler's Request Switching technology can be applied to SSL traffic to ensure the secure delivery of web applications without degrading end-user performance.

1.5.2.2 Secure Remote Access

NetScaler’s Secure Remote Access capabilities allow enterprises to provide their employees, partners and customers with instant access to all authorized applications, files or data from a standard Web browser. By using SSL as the underlying protocol, it requires no incremental client software and no changes to servers or LANs.

In addition to providing an internal LDAP directory, the AAA module of this SSL VPN integrates with other enterprise directories such as RADIUS, Microsoft Active Directory and other external LDAP servers.

1.5.2.3 Distributed Denial of Service Attack (DDoS) Defense

The NetScaler 9000 Series product line takes network security to a new level by intelligently stopping malicious attacks before they reach the servers without affecting network and application performance. The NetScaler 9000

system identifies legitimate clients and elevates their priority, leaving suspect clients unable to consume resources at a rate that would otherwise cripple a site.

The NetScaler 9000 system provides application-level protection from other malicious attacks including SYN flood attacks, pipeline, teardop, land, fraggle, and zombie connection attacks. The NetScaler 9000 system aggressively defends against these types of attacks by preventing the allocation of server resources for these connections. This insulates servers from the overwhelming flood of packets associated with these events.The NetScaler 9000 system also protects network resources from ICMP based attacks by using a variety of intelligent mechanisms such as ICMP rate limiting and aggressive ICMP packet inspection.

The NetScaler 9000 system also performs strong IP reassembly, drops a variety of suspicious and malformed packets, and applies Access Control Lists (ACLs) to site traffic for further protection.

1.5.2.4 Content Filtering

Content filtering provides protection from malicious attacks for web sites at the layer 7 level. The NetScaler 9000 system inspects every incoming request according to user-configured rules, which are based on HTTP headers. The NetScaler 9000 system then performs the corresponding action to each rule as configured by the user. Actions may include resetting the connection, dropping the requests or sending an error message. This allows the system to screen unwanted requests from the protected server and reduce the exposure of the server to potential attacks.

The NetScaler 9000 system's content filtering feature can also be used to shield against intrusion attempts by analyzing HTTP GET and POST requests and filtering out known bad signatures. This mechanism can be used to defend against HTTP-based attacks such as variants of Nimda and Code Red virus.

1.5.2.5 Surge Protection

During peak traffic periods, the NetScaler 9000 system maintains the capacity of a server or cache by regulating the flow of user requests to servers and controlling the number of users that can simultaneously access them. By controlling the rate at which connections are established, the NetScaler 9000 system blocks the surge from being passed to the server and prevents the site from becoming overloaded. User requests that arrive after the server has reached its configured capacity are queued at the NetScaler 9000 until

resources become available. Because the surge of traffic has not been passed to the server, the server resources are preserved assuring all users of a better and more consistent experience.

1.5.2.6 Priority Queuing

When a site is in a surge condition and clients are contending for access to server resources, the NetScaler 9000 system can prioritize user request to ensure that the most important traffic is serviced first. Priority can be established based on requested URLs, cookies or a variety of other factors. The NetScaler 9000 system places requests in a three-tier queuing system based on their configured priority, enabling business-critical transactions to flow smoothly even if unexpected surges or site attacks occur. Priority queuing enables continuous delivery of the most important requests, even when a site is under attack or overloaded.

1.5.2.7 SureConnect™

SureConnect ensures application responsiveness even when servers are working at capacity or applications are experiencing processing delays. By providing real-time estimates of Internet response times, interactive priority queuing, and guaranteed content delivery, SureConnect can dramatically improve the real and perceived availability of a site by eliminating the gap between your customer's expectations and their browsing experience.

1.5.3 Application Optimization Features

The NetScaler 9000 system includes the following traffic optimization features:

- Compression
- TCP Off Load
- Client Keep-alive
- TCP Buffering
- Consolidated Logging
- Application Caching
- TCP Compression

1.5.3.1 Compression

The NetScaler 9000 system provides transparent compression for HTML and text files. The typical 4:1 compression yields up to 50% reduction in bandwidth requirements out of the data center. This also results in significantly improved end-user response time by reducing the amount of data that must be delivered to the browser.

1.5.3.2 TCP Offload

To optimize server throughput and improve response times, the NetScaler 9000 system eliminates server-processing bottlenecks by offloading the TCP connection burden from servers and caches and by enabling long-lived persistent connections across the Internet. This significantly reduces the connection burden on servers and accelerates static, dynamic and interactive content.

1.5.3.3 Client Keep-alive

The NetScaler 9000 system further reduces WAN latency by maintaining persistent connections with the client. Typically, a server with Keep-alive disabled, will close a connection as soon as it has delivered an object. This means a client must open and close many connections to download a complete page. The NetScaler 9000 system keeps the connection open to the client and then switches new requests onto reusable connections to the server, thus eliminating much of the overhead and delay that the client would experience.

When the server closes the connection, the NetScaler 9000 system keeps the client-side connection (between the client and the NetScaler 9000) open. This allows multiple client requests to be serviced on a single client connection. In the absence of this feature, a client would have to open a new connection for every request to the server. Instead, client keep-alive saves packet round trips associated with connection establishment and closure, reducing the time to complete each transaction.

1.5.3.4 TCP Buffering

The NetScaler 9000 system also allows significant scaling of server infrastructure and improves application response times in connection-limited, higher packet loss situations by treating all clients as if they were connected at LAN speeds. This is made possible by buffering data from the server onto the NetScaler 9000 system, relieving the server from slow clients and quickly

freeing up resources for new requests. This also permits the NetScaler 9000 system to optimize the TCP parameters for each of these clients and fully manage any retransmissions of dropped packets.

1.5.3.5 Consolidated Web Logging

The NetScaler 9000 system's web server logging feature offloads the logging function from a server or cache to central location. When configured for consolidated web server logging, the NetScaler 9000 system tracks client activity on all of the web servers or virtual web servers to which it is connected. It can record client activity in a single file or in separate log files. The NetScaler 9000 system supports three different log file formats for displaying data in the log files: W3C Extended log file format, NCSA Common log file format or Custom log format.

1.5.3.6 Application Caching

NetScaler's Application Caching option helps to optimize the delivery of web content and application data by providing a fast in-memory HTTP/1.1 and HTTP/1.0 compliant web cache for both static and dynamic content. This on-board cache stores the results of incoming application requests even when an incoming request is secured or the data compressed, and then reuses the data to fulfill subsequent requests for the same information. By serving data directly from the on-board cache, the NetScaler 9000 system can eliminate the need to funnel static and dynamic content requests to server infrastructure – offloading servers and reducing page regeneration times.

1.5.4 Application Switching Features

The NetScaler 9000 system includes the following traffic switching features:

- Load Balancing
- Content Switching
- Cache Redirection
- Global Server Load Balancing
- Link Load Balancing

1.5.4.1 Load Balancing

NetScaler's load balancing feature manages traffic at the request level resulting in more uniform traffic distribution across systems, compared to the

conventional approach of distributing connections among these systems. Load balancing decisions are based on a variety of policies including round robin, least connections, weighted least bandwidth, weighted least packets, minimum response time and hashing (based on URL, domain source IP or destination IP).

As both TCP and UDP protocols are supported, all HTTP, HTTPS, UDP, DNS, FTP, NNTP, and general firewall traffic can be load balanced. In addition, The NetScaler 9000 system can maintain session persistence based on source IP, cookie, server, group, or SSL session. The NetScaler 9000 system also allows users to apply custom Extended Content Verification (ECV) to servers, caches, firewalls and other infrastructure devices to ensure that these systems are functioning properly and providing the right content to users. The NetScaler 9000 system can also perform other health-monitoring checks via ping, TCP, or HTTP URL.

1.5.4.2 Content Switching

Using a powerful policy engine, the NetScaler 9000 system switches individual content requests to the server best able to respond. Site rules can be configured based on URL and any combination of HTTP headers. This allows switching decisions to be made based on user and device characteristics such as who the user is, what type of agent they are using, and the content they request.

1.5.4.3 Cache Redirection

Cache redirection manages the flow of traffic to a reverse proxy, transparent, or forward proxy cache farm. It inspects all requests, identifies non-cacheable requests and then sends those requests directly to the origin servers over persistent connections. By intelligently, redirecting non-cacheable requests back to the origin web servers, the NetScaler 9000 system frees cache resources and increases cache hit rates while reducing overall bandwidth consumption and response delays for these HTTP requests.

1.5.4.4 Global Server Load Balancing

The NetScaler 9000 system extends its traffic management capabilities to include distributed Internet sites and global enterprises. Whether installations are spread across multiple network locations or multiple clusters in a single location, the NetScaler 9000 system maintains availability and distributes

traffic across them. Intelligent DNS decisions are then made to prevent users from being sent to a site that is down or overloaded.

1.5.4.5 Link Load Balancing

To further optimize network performance and to ensure business continuity, the NetScaler 9000 system can load balance multiple WAN links and provide link fail over. This link load balancing feature ensures that network connections remain highly available by applying intelligent traffic control and health checks to efficiently distribute traffic across upstream routers. It identifies the best WAN link to route both incoming and outbound traffic based on policies and network conditions and protects applications against WAN or Internet link failure by providing rapid fault detection and fail over.

1.6 Technical Support and Resources

In addition to the Installation and Configuration Guide and Command Reference, technical assistance is also available in the following locations:

1.6.1 Customer Support

Use the following details for assistance with NetScaler 9000 system products and to contact the NetScaler Customer Support Center.

Website	www.netscaler.com
Phone	USA 1-408-678-1601 Or 1-866-NETSCALER
E-mail	support@netscaler.com

1.6.2 Release Notes

The release note for the current version of the NetScaler 9000 system is available in the package you received with the product. The release notes,

which contains the latest information for the version of software that is shipped with your system, includes:

- New features and enhancements
- Fixes and work-arounds for known issues

Chapter 2
Installation, Configuration and Management

This chapter describes how to install, configure and manage the Product Name (short) system.

Topics included in this chapter are:

- System Models
- LCD Monitor in NetScaler 9000 System
- Installing the NetScaler 9000 System
- Configuring the NetScaler 9000 System
- Maintaining the NetScaler 9000 System
- Managing the NetScaler 9000 System
- Understanding NetScaler License Keys
- Autodetect Service

2.1 System Models

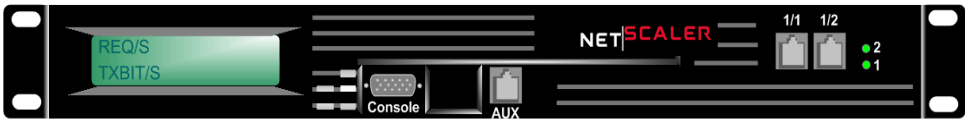
The 9400 and 9200 models have identical hardware platforms. In this chapter, we will use NetScaler 9400 to refer to both models unless otherwise noted. Similarly, the 9800 and 9600 have identical hardware platforms. In this chapter, we will use 9800 to refer to both models unless otherwise noted.

Note: The 9x00-N variation of each system type has internal hardware differences but the external appearance is identical.

2.1.1 NetScaler 9400

The NetScaler 9400 is a 1U unit that supports Fast Ethernet and has one GB of memory. Figure 2-1 shows this model.

Figure 2-1 The NetScaler 9400 1U unit that supports Fast Ethernet and has one GB of memory.



- **Ports**
  - **a.** Two 10/100Base-T network interfaces (labeled `1/1` and `1/2`)
  - **b.** One auxiliary interface for future use (labeled AUX)
  - **c.** Serial Console (9600 baud, 8 bits, 1 stop bit, No parity)

- **LEDs**

  - The LED labeled `1` on the unit corresponds to the port labeled `1/1`.
  - The LED labeled `2` on the unit corresponds to the port labeled `1/2`.

  When lit, they indicate the following:

  - Green indicates the link is established for the corresponding port.
  - Yellow indicates that the corresponding port is active (transmitting or receiving traffic).

2.1.2 NetScaler 9800-SX

The NetScaler 9800-SX is a 2U unit that supports fiber Gigabit Ethernet and has two GB of memory. Figure 2-2 shows this model.

Figure 2-2 The 9800-Secure Application Switch

- **Ports**
  - **a.** Four 1000Base-SX network interfaces (labeled `1/1`, `1/2`, `1/3`, and `1/4`)

b. One 10/100/1000Base-T network interface (labeled `0/1`)

c. Serial Console (9600 baud, 8 bits, 1 stop bit, No parity)

- **LEDs**

  When the LEDs on the NetScaler 9800-SX are lit, they indicate the following:

  - LED labeled `1000`: The corresponding port has been established for 1000Base-SX.
  - LED labeled `ACT`: The corresponding port is active (receiving or transmitting traffic).

2.1.3 NetScaler 9800-T

The NetScaler 9800-T is a 2U unit that supports copper Gigabit Ethernet and has two GB of memory. Figure 2-3 shows this model.

Figure 2-3 NetScaler 9800-T System

- **Ports**

  The NetScaler 9800-T unit has the following ports:

  - Four 10/100/1000Base-T network interfaces (labeled `1/1`, `1/2`, `1/3`, and `1/4`)
  - One 10/100/1000Base-T network interface (labeled `0/1`)
  - Serial Console (9600 baud, 8 bits, 1 stop bit, No parity)

- **LEDs**

  When the LEDs on the NetScaler 9800-T are lit, they indicate the following:

  - LED labeled `1000`: The corresponding port has been established for 1000Base-T.

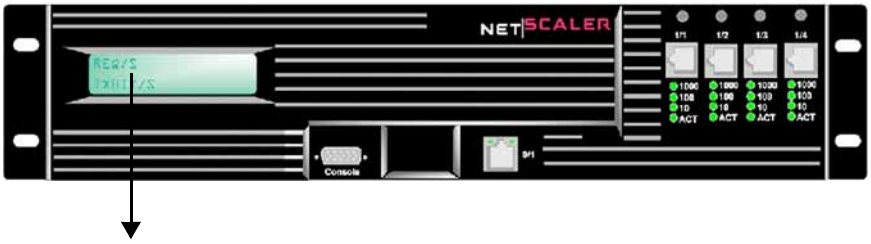
- LED labeled `100`: The corresponding port has been established for 100Base-T.
- LED labeled `10`: The corresponding port has been established for 10Base-T.
- LED labeled `ACT`: The corresponding port is active (receiving or transmitting traffic).

2.2 LCD Monitor in NetScaler 9000 System

The NetScaler 9000 Series products have a Liquid Crystal Display (LCD) on its faceplate. This LCD displays real-time statistics, diagnostic information and active alerts.

Note: By default, the refresh rate of the screen is 3 seconds and this value can be re-configured using the Product Name (short) system LCD Program Options.

Figure 2-4 NetScaler 9000 system 9800-T



2.2.1 Overview

As the dimension of the LCD is limited (two lines of 16 characters), the display information flows through a sequence of screens. Each screen displays a piece of information about some part of a specific NetScaler 9000 system function.

2.2.2 NetScaler 9000 system LCD Back Light

- The NetScaler 9000 system LCD has a neon backlight that starts blinking when there is an active alert. If the display information is more than one screen then it blinks at the beginning of each display screen.
- When the Product Name (short) system shuts down the backlight remains ON exactly for one minute and then automatically turns OFF.
- If the LCD displays **`OUT OF SERVICE`** message, this indicates that the Product Name (short) system has been stopped (with or without errors).

2.2.3 Display Information

The display information on the Product Name (short) system LCD can be divided into two categories:

- Special Display Screens: this information is displayed for very specific scenarios.
- Regular Display Screens: this information is displayed when the Product Name (short) system is in active mode.

Note: By default, the refresh rate of the screen is 3 seconds and this value can be reconfigured using the Product Name (short) system's LCD Program Options. Refer to "NSLCD program options" on page 12 for more information.

2.2.4 Special Display Screens

◆ **Power Up screen**

This screen is displayed immediately after the Product Name (short) system is switched **ON**.

Figure 2-5 Power-on display in LCD

1 The first line in the display shows the company name.

2 The second line in the display shows the Product Name (short) system's power status.

Note:

1. The message on this screen can be customized using a shell command. For more information, refer to "NSLCD program options" on page 12.
2. This Power Up message is displayed until the boot process is successfully completed.

- **Start Up Screen**

  This screen is displayed only for few a seconds after the Product Name (short) system successfully starts its operation.

Figure 2-6 Start-up display in LCD

1 The first line in the LCD displays the product name.

2 The second line in the LCD displays the software version and build number.

- **Out of Service Screen**

  This screen is displayed when the NetScaler 9000 system stops functioning. The main reasons for the NetScaler 9000 system to stop functioning are:

  - Regular NetScaler 9000 system shut down
  - Operational errors
  - If the NSLCD program is stopped by using the **`kill`** command.

Figure 2-7 Out of Service display in LCD

1. The first line displays the message.
2. The second line displays the IP address of the NetScaler 9000 system that has stopped.

Note: If the "Out of Service" error message is not displayed on the NetScaler 9000 system LCD, check the NetScaler 9000 system console for more information on why NetScaler 9000 system is not functioning.

2.2.5 Regular Display Screens

- **Configuration Screen**

  The NetScaler 9000 system LCD displays this configuration information as shown in the following figure:

Figure 2-8 Configuration display in LCD

1. The first line displays:
   - **a.** The NetScaler 9000 system status as:
   - **`Pri`**: Indicates that the NetScaler 9000 system box is in Stand-alone mode or indicates that the NetScaler 9000 system is the Primary node in a High Availability pair.

   —Or—

   - **`Sec`**: Indicates that the NetScaler 9000 system is the Secondary node in a High Availability pair.

   b. The system uptime of the NetScaler 9000 unit in the `HH:MM` format.

c. The NetScaler 9000 system Alert status:

- For a known alert, the alert name is shown in the following figure:

Figure 2-9 LCD displaying Known Alert

- For an unknown alert, a message 'Alert' is displayed as shown in the following figure:

Figure 2-10 LCD displaying Unknown Alert

2 The second line displays the IP address of the NetScaler 9000 system.

◆ **HTTP Statistic Screen**

The NetScaler 9000 system LCD displays the HTTP statistics as shown in the following figure:

Figure 2-11 LCD displays HTTP Statistics

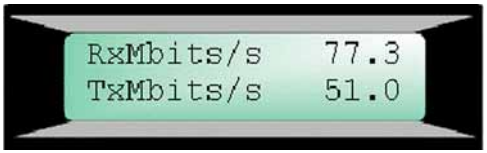
1 The first line displays the rate of HTTP GETs per second.

2 The second line displays the rate of HTTP POSTs per second

◆ **Network Traffic Statistic screen**

The NetScaler system LCD displays the Network Traffic statistics as shown in the following figure:

Figure 2-12 LCD displays Network Traffic Statistics



1. The first line displays the rate of the Received data in Megabits per second.
2. The second line displays the rate of Transmitted data in Megabits per second.

- **CPU Load, Memory and Connections Screen**

  The NetScaler 9000 system LCD displays the CPU Load, Memory and the Total Connections statistics as shown in the following figure:

Figure 2-13 LCD displays CPU Load, Memory and Total Connections statistics

1. The first line displays the following information:
   - CPU utilization in percentage
   - memory utilization in percentage
2. The second line displays the number of **Server / Client** connections.

Note: If the **Server / Client** total connections exceed 99,999 for server connections and 999,999 for client connections then the number of connections are displayed in thousands (with a suffix 'K').

- **Port Information**

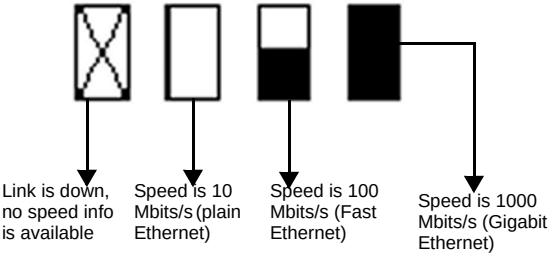
  The LCD in the NetScaler 9000 system is divided into four quadrants. Every quadrant contains a specific symbol and have five fixed spaces for per port information. The spaces are numbered from left to right as **`0/1, 1/1, 1/2, 1/3, 1/4`** corresponding to the port numbering schema.

Note: The NetScaler 9400 system has only two ports **1/1** and **1/2** and hence uses only second and third space to display the port's information.

1 *First Quadrant* (displayed in the Top Left corner as symbol **S**)

This quadrant shows the *port speed information*. The speed displayed is encoded in special symbols as shown in the following figure:

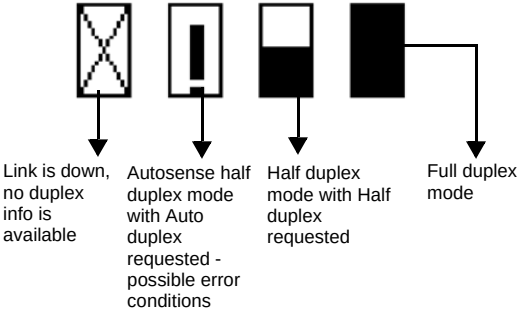
Figure 2-14 First Quadrant: Port Speed Information


Link is down, no speed info is available
Speed is 10 Mbits/s (plain Ethernet)
Speed is 100 Mbits/s (Fast Ethernet)
Speed is 1000 Mbits/s (Gigabit Ethernet)

2 *Second Quadrant* (displayed in the Bottom Left corner as symbol **D**)

This quadrant displays the *port duplex* information. The duplex status displayed is encoded in special symbols as shown in the following figure:

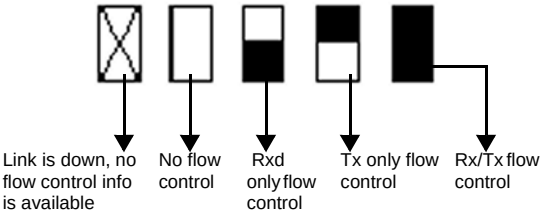
Figure 2-15 Second Quadrant: Port Duplex Information


Link is down, no duplex info is available
Autosense half duplex mode with Auto duplex requested - possible error conditions
Half duplex mode with Half duplex requested
Full duplex mode

3 Third Quadrant (displayed in the Top Right corner as symbol **F**)

This quadrant displays the *port flow control* information. The flow control status displayed is encoded in special symbols as shown in the following figure:

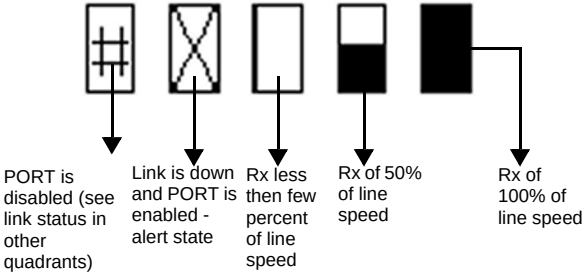
Figure 2-16 Third Quadrant: Port Flow Control Information


Link is down, no flow control info is available
No flow control
Rxd only flow control
Tx only flow control
Rx/Tx flow control

4 Fourth quadrant (displayed in the Bottom Right corner as symbol **R**)

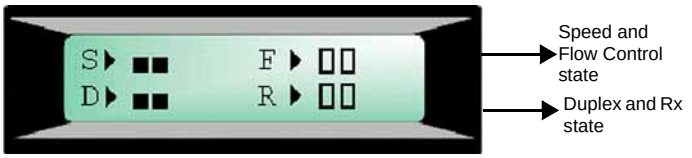
This quadrant displays the PORT Receive (Rx) statistics and PORT Enable state. These statistics are encoded in special symbols as shown in the following figure:

Figure 2-17 Fourth Quadrant: Port Receive Statistics Information


PORT is disabled (see link status in other quadrants)
Link is down and PORT is enabled - alert state
Rx less then few percent of line speed
Rx of 50% of line speed
Rx of 100% of line speed

For example

The NetScaler 9400 system LCD screen with two interfaces **1/1** and **1/2** is shown below. Both the interfaces are in 100 Mbit / Half Duplex / No Flow Control / Rx Idle mode.



2.2.6 NSLCD program options

The NetScaler 9000 system LCD (NSLCD) program has the following program options available will help you to control the information displayed.

Note: The NetScaler 9000 system startup script uses appropriate options hence customizing the options may be used for very specific requirements.

Table 2-1 List of NSLCD Commands

Option	Description	NSLCD command
-k	Starts the NSLCD in background for NetScaler 9000 system status monitoring	**/netscaler/nslcd -k**
-h	Displays the help screen	**/netscaler/nslcd -h**
-t SEC	Sets the refresh rate time in seconds. *Default refresh rate is 3* seconds.	**/netscaler/nslcd -t SEC**
-b MIN	Sets the back light time-out in minutes *Default value for the back light timeout is 1 minute*	**/netscaler/nslcd -b MIN**
-S	Enables serial communications.	**/netscaler/nslcd -S**
-A	Enables alternate device. This option must be used with `-Q` option.	**/netscaler/nslcd -A**

Option	Description	NSLCD command
-Q	Queries LCD type and version. If the type and version are not correct then the NSLCD will halt with an error message.	**/netscaler/nslcd -Q**
-K	• Runs the NSLCD in loop but not as a daemon. • Used to tune up the LCD indication.	**/netscaler/nslcd -K**
-i	Skips the introduction screen.	**/netscaler/nslcd -i**

2.3 Installing the NetScaler 9000 System

This section describes how to install the NetScaler 9000 system on to your network. The steps involved in installing the system are:

- Environment Planning
- Pre-Installation Checklist
- Installing the NetScaler 9400 System or Installing NetScaler 9800 System

2.3.1 Environment Planning

This section describes the environments in which the NetScaler 9000 system can be deployed. Before you install the NetScaler 9000 system, use this information to help you determine an appropriate environment for your installation.

2.3.1.1 Single Subnet

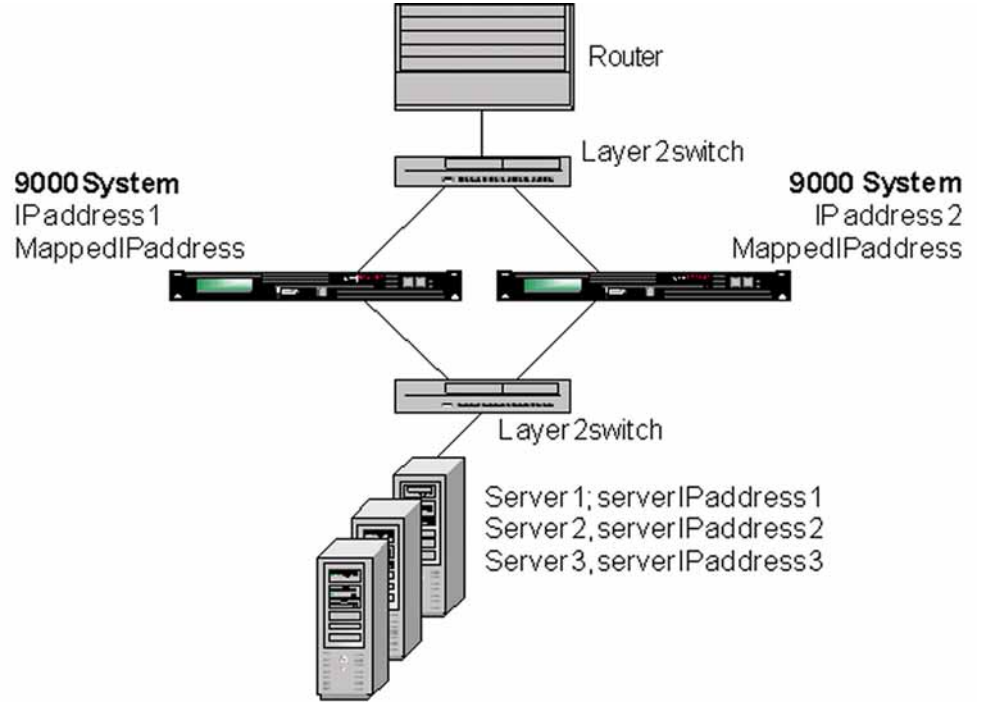
In this type of environment, the NetScaler 9000 system's IP address, mapped IP address (MIP) and the server's IP address are on the same subnet. The NetScaler 9000 system can be deployed in one-arm or two-arm mode.

- **Two-Arm Mode (Inline), High Availability**

  Figure 2-18 on page 15 shows a single subnet environment where the NetScaler 9000 system is in a high availability setup, placed between two layer 2 switches in a two-arm configuration.

  The two NetScaler 9000 systems with their IP addresses, mapped IP addresses and the servers with IP addresses are on the same subnet.

Figure 2-18 NetScaler 9000 system in High Availability, Two-Arm Mode (Single Subnet Environment)

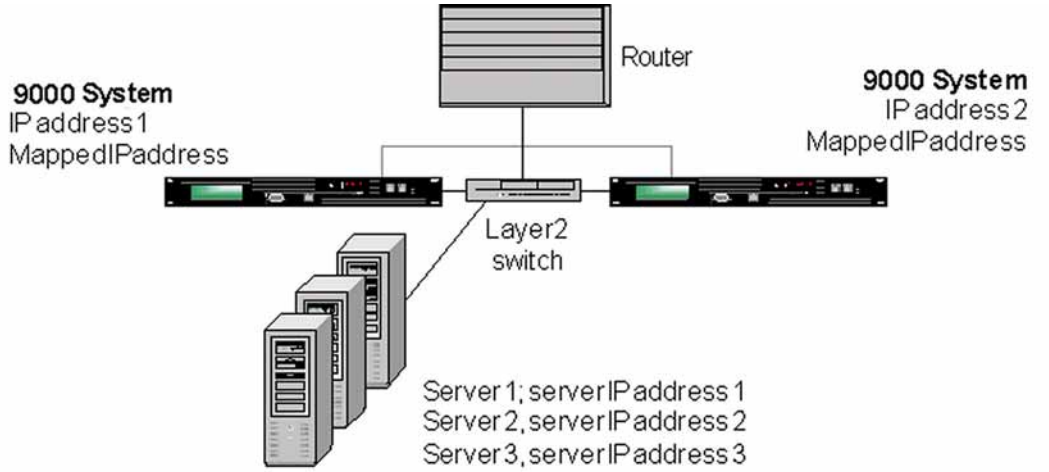


All of the IP addresses shown in the example are in the same subnet.

- **One-Arm Mode, High Availability**

  Figure 2-19 on page 16 shows a single subnet environment where the NetScaler 9000 system is in a high availability setup in a one-arm mode. In this type of deployment, the client must access the servers though a VIP configured on the NetScaler 9000 system.

Figure 2-19 NetScaler 9000 system in High Availability and One-Arm Mode (Single Subnet Environment)



All of the IP addresses shown in the example are in the same subnet.

- **Stand-Alone**

  To use a NetScaler 9000 system in a single subnet environment and in a stand-alone mode (not in high availability setup), the setup slightly varies from that shown in Figure 2-18 and Figure 2-19. In this case, there is only one NetScaler 9000 system instead of two NetScaler 9000 systems.

2.3.1.2 Multiple Subnets

In this type of environment, the NetScaler 9000 system's IP address, its mapped IP address (MIP), and the server's IP address are on different subnets. The NetScaler 9000 system can be used in one-arm or two-arm mode.

Depending on whether the servers are on private (non-routable) subnets, the NetScaler 9000 system can be used either in a public-public or public private type of multiple subnet environments.

Note: If the NetScaler 9000 system is the default router for the servers, then the layer 2 mode can be disabled.

- **Public-Public**

  In this environment, the real servers behind the NetScaler 9000 system are on a publicly routable IP subnet. Unlike the public-private environment (described in the next section), you do not need to configure the NetScaler 9000 system as the default router of the real servers.

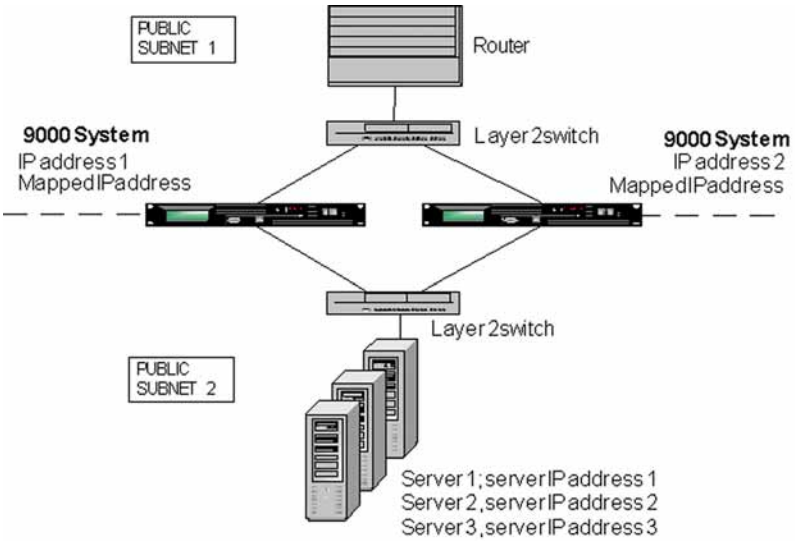
  Figure 2-20 on page 17 shows a public-public, multiple subnet environment where the NetScaler 9000 system is in a high availability setup, placed between two layer 2 switches in a two-arm configuration. The dashed line shows the separation of two public subnets.

  The following applies to this environment:

  - Virtual IP addresses (VIPs) configured in the NetScaler 9000 system are on a public subnet.
  - The two NetScaler systems, their IP addresses and the mapped IP address are on public subnets.
  - The servers and their IP addresses may be either in the same or different public subnets.

  This environment can be varied to yield a one-arm mode configuration with or without high availability.

Figure 2-20 NetScaler 9000 system in High Availability and Two-Arm Mode (Multiple Subnet Environment)



- **Public-Private**

  When load-balancing a server farm, it may be desirable to hide the IP addresses of the real servers. This can be accomplished by placing the servers on non-routable IP subnets.

  Although no router or gateway is usually placed between the NetScaler 9000 system and server farm, the router or gateway can be placed there if required .

  In this environment, the servers must be configured with the NetScaler 9000 system as the default router.

  Depending on whether the NetScaler 9000 system needs to perform network address translation (NAT) the subnet with the servers should be configured for reverse network address translation (NAT) in the NetScaler 9000 system. For more information on configuring RNAT in NetScaler 9000 system, see "VLANs Support in Chapter 13".

  This environment is the same as that shown in Figure 2-20 (i.e. the high availability, two-arm mode), except the upper part is a public subnet and the lower part consists of private subnets.

  The following applies to this environment:

  - Virtual IP addresses (VIPs) configured in the NetScaler 9000 system are on a public subnet.
  - The two NetScaler 9000 systems, their IP addresses and the mapped IP address are on public or private subnets.
  - The servers and their IP addresses may be either in the same or different private subnets.

  This environment can be varied to yield a one-arm mode with or without high availability.

2.3.2 Pre-Installation Checklist

Before installing the NetScaler 9000 system, use the following check list to ensure that you have all of the hardware and software items:

2.3.2.1 Hardware

1. NetScaler 9000 system
2. Brackets to hold NetScaler 9000 system
3. RJ-45-to-RJ-45 Serial Cable

4. One or two AC power cable(s)
5. Two RJ-45-to-DB-9 adapters
6. RJ-45-to-DB-25 adapter
7. Packet of screws
8. Ethernet cables (not supplied)
9. One or two power outlets
10. Rack space
11. Free switch ports to connect to the NetScaler 9000 system

2.3.2.2 Software

1. IP addresses
    - One or two NetScaler IP addresses [NSIP] (In HA mode you require two unique NetScaler IP addresses)]
    - Appropriate password choices for the **`root`**, **`nsmaint`**, and **`nsroot`** account. As part of the deployment process, these three account passwords must be changed.

    Note: In HA mode, when you change the password of the **`nsroot`** user account, make sure you change it to the same password on both nodes of the HA pair as password synchronization is required.

    - Mapped IP[MIP]
    - IP address for the NetScaler 9000 system's default router
    - Additional subnet/VLAN IP addresses as needed
2. Additional IP address(s) for any virtual servers (VIPs) that needs to be configured

Note: The NetScaler 9000 system supports any combination of 5000 virtual servers and configured services.

3. For SNMP access to NetScaler 9000 system, you must have
    - One Community Name
    - IP address of management station

2.3.3 Installing the NetScaler 9400 System

To install and connect the NetScaler 9400 system into your network:

1. Place the NetScaler 9400 system into the rack.
2. Attach the NetScaler 9400 system to the rack by securing the screws provided, into the holes on each side of the unit's front.
3. Connect the Ethernet cable(s).

   You must provide these cables. These are connected from the Ethernet ports on the front of the NetScaler 9400 system to the Ethernet ports on the devices on your network.

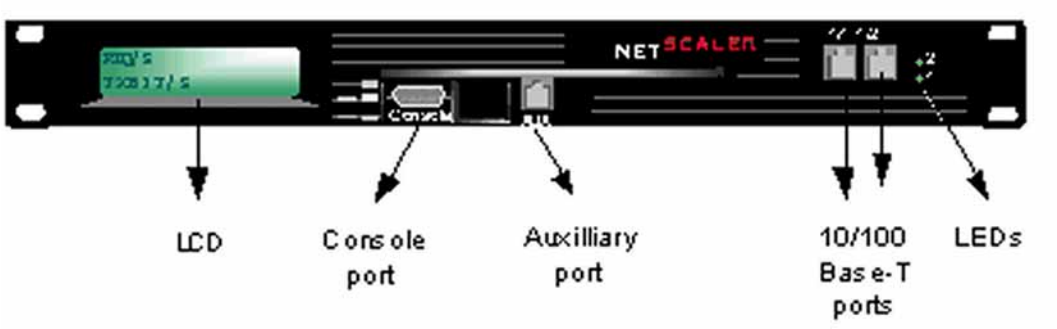
   a. Connect one end of a cable to the port labeled `1/1` on the front of the NetScaler 9400 system (see Figure 2-21 on page 21 for the location of this port), then connect the other end to the Ethernet port on the switch.

   b. (Optional) Connect one end of another cable to the port labeled `1/2` on the front of the NetScaler 9400 system (see Figure 2-21 on page 21 for the location of this port), then connect the other end to the Ethernet port on the switch.

WARNING! Make sure not to create a network loop — this results if you connect the cable in step 3a and the cable in step 3b to the same switch or VLAN.

Note: If current configuration requires only one Ethernet port to be used then any of ports 1/1 or 1/2 could be used. It is always good idea to DISABLE the unused port(s) (it's also mandatory in HA configuration).

Figure 2-21 Front panel of NetScaler 9400

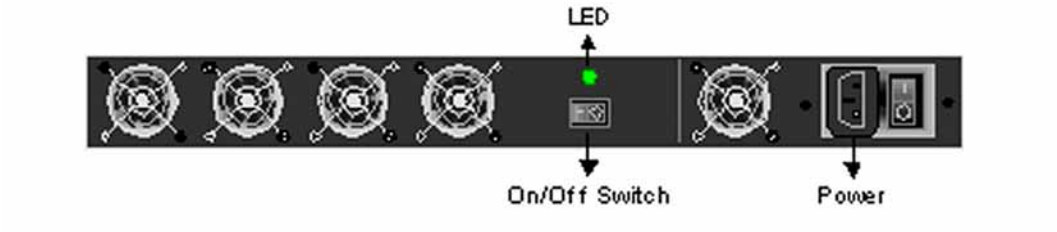


4. Connect a terminal (which can be a computer supporting VT100 terminal emulation) to the console port on the front of the unit.

Note: The terminal that you supply must have a baud rate and character format configured to 9600 baud, 8 data bits, 1 stop bit and no parity.

5. Power-on the NetScaler 9400 system.

Figure 2-22 Back panel of NetScaler 9400



   a. Plug-in the power cord that comes with the unit on the back of the NetScaler 9400 system. See the above figure.
   b. Depress the `On/Off` switch present at the back of the unit.

      The green LED appears lit.

WARNING! After the initial power-on, to power-off the NetScaler 9400 system follow the steps as described in the "Powering-Off the NetScaler 9000 system" on page 44.

NetScaler 9400 system operation starts.

- For initial configuration of the NetScaler 9400 system (first time configuration), perform the procedure as described in the *Configuring and Starting the NetScaler 9000 system for the First Time* section in this chapter.
- If you are reconfiguring the NetScaler 9000 system, perform the procedure in the *Reconfiguring the NetScaler 9000 system* section in this chapter.

2.3.4 Installing NetScaler 9800 System

Figure 2-23 on page 23 shows the NetScaler 9000 system NetScaler 9800-SX fiber unit.

Figure 2-24 on page 23 shows the NetScaler 9000 system NetScaler 9800-T copper unit.

To install and connect the NetScaler 9000 system into your network:

1. Place the NetScaler 9000 system into the rack.
2. Attach the NetScaler 9000 system to the rack by securing the screws provided, into the holes on each side of the unit's front.
3. Connect the Ethernet cables.

   You must provide these cables (copper or fiber ones depending on the NetScaler 9000 system used). These are connected from the Ethernet ports on the front of the NetScaler 9000 system to the Ethernet ports on the devices on your network.

   a. Connect the end of an Ethernet cable to one of the ports labeled `1/1`, `1/2, 1/3` or `1/4` on the front of the NetScaler 9000 system (see Figure 2-23 for port locations), and then connect the other end to the port on the switch. It is not recommended to use the port 0/1 until you have other choices.

   b. Connect the end of another cable to any of the available ports labeled `1/1`, `1/2`, `1/3` or `1/4` on the front of the NetScaler 9000 system (see Figure 2-23 for port locations), and then connect the other end to the port on the switch.

Note: Make sure not to create a network loop — this results if you connect the cable in step 3a and the cable in step 3b to the same switch.

In case when current configuration requires less than five ports then any of five available ports could be used (based on Ethernet technology used). It is good idea to DISABLE all unused ports through software (it is mandatory for HA configuration).

Figure 2-23 Front panel of NetScaler 9800-SX

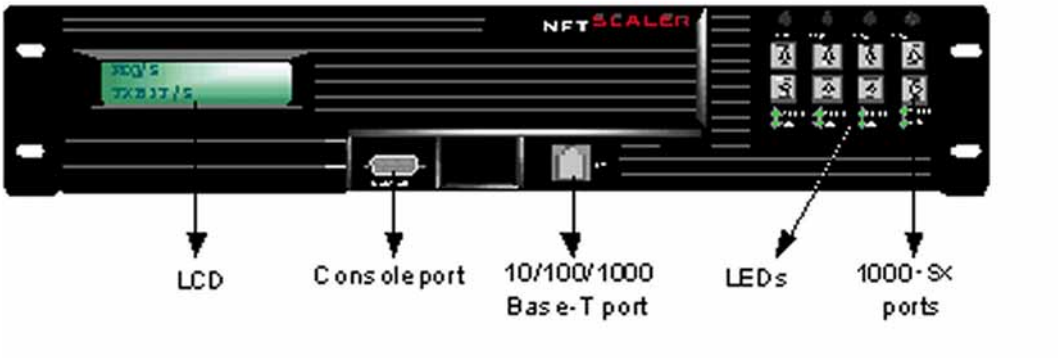
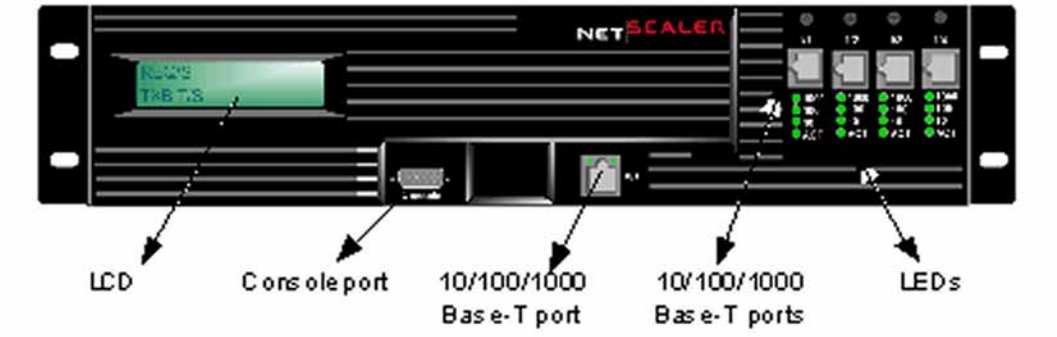


Figure 2-24 Front of NetScaler 9000 system NetScaler 9800-T

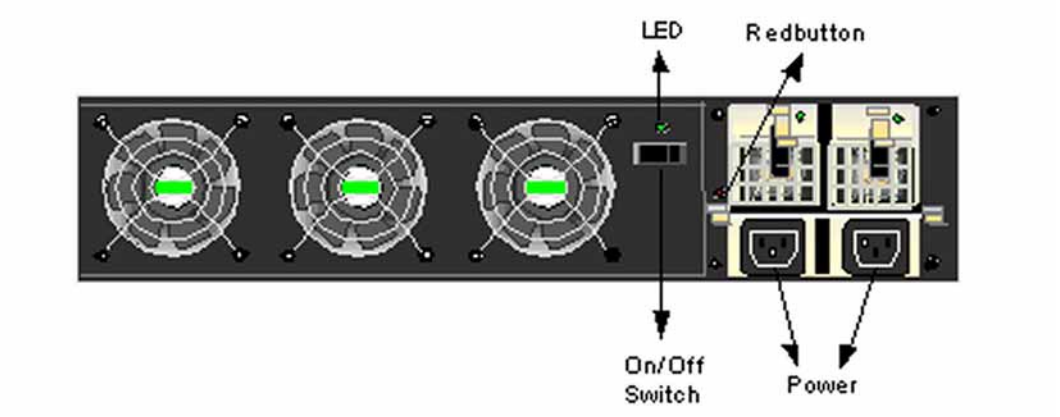


4. Connect a terminal (which can be a computer supporting VT100 terminal emulation) to the console port on the front of the unit.

Note: The terminal that you supply must have a baud rate and character format configured to 9600 baud, 8 data bits, 1 stop bit, and no parity.

5. Power-on the NetScaler 9000 system. Refer to Figure 2-25 on page 24 for the location of the **ON/OFF** button.

Figure 2-25 Back panel of NetScaler 9800-T or NetScaler 9800-SX system



   a. Plug in the ***two*** power cords that come with the unit into the back of the NetScaler 9000 system (see Figure 2-25 for the location of the power).

      MAKE SURE that you plug in BOTH power cords.

      For 2U NetScaler systems with only one power supply cable plugged in, the system will emit a high pitched alert. This alert can be shut off in one of three ways, depending upon the hardware version.

      1. If present, press the small red button at the back of the box near the power plugs. This will have to be done each time the system is powered on.

      2. If the red button on the rear of the case is not present, check on the front of the unit around the LCD screen. You will need to remove the faceplate to see the button for silencing the alarm.

      3. If neither of these buttons are present on the unit, power cables must be used. The alarm cannot be manually overridden on these units.

   b. Turn the switch to the right of the three fans on the back of the unit to the on position.

The green LED above the switch lights and stays lit.

Note: After the initial power-on, turn power off only, as described in the Powering-Off the NetScaler 9000 system on Page '44' in this chapter.

2.3.5 Installation Tips

- If you are setting up the NetScaler 9000 system for the first time, follow the steps given in "Initial Configuration of NetScaler 9000 System" on page 27 of this chapter.
- If you are reconfiguring the NetScaler 9000 system, follow the steps given in the "Reconfiguring the NetScaler 9000 system" on page 43 of this chapter.

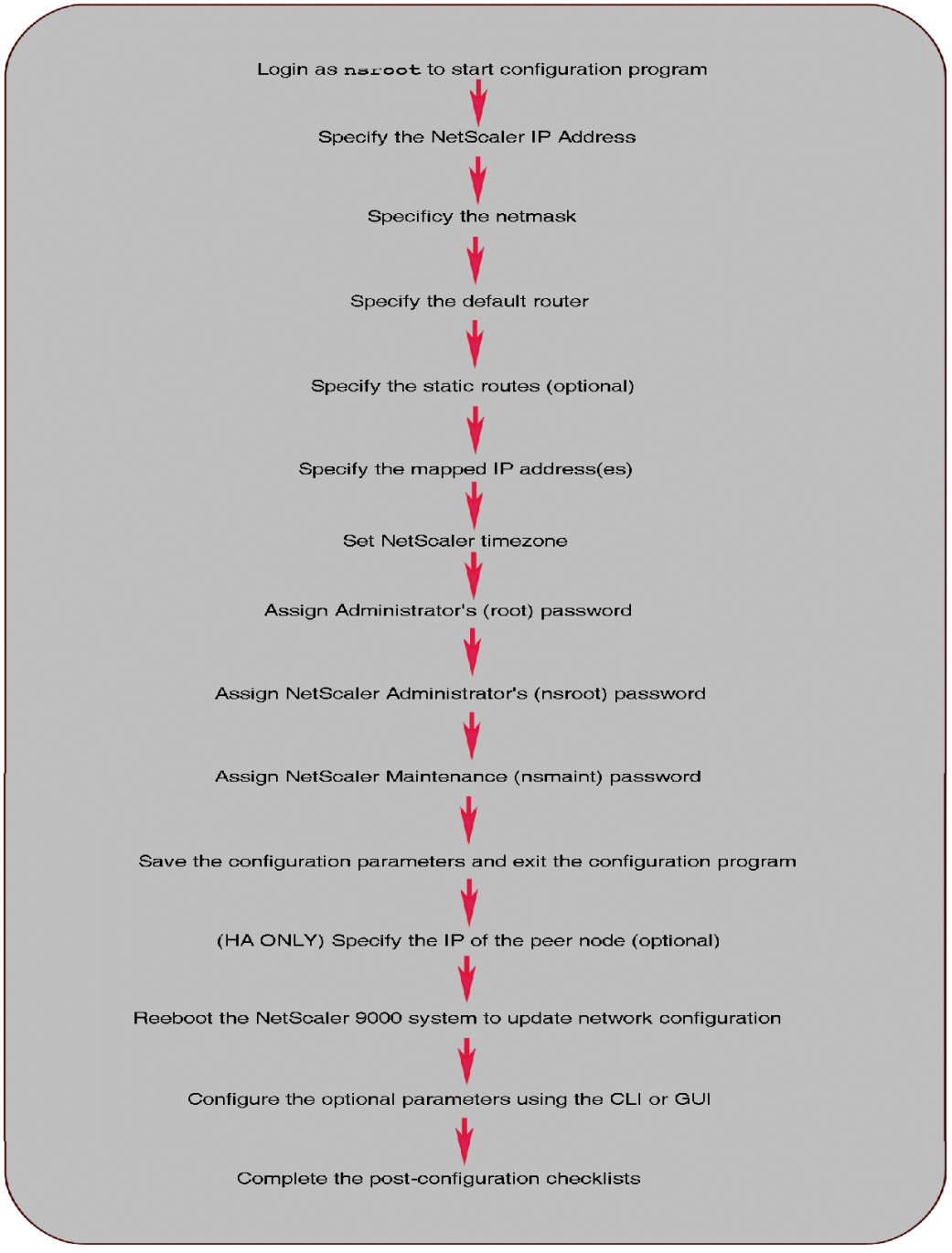
2.4 Configuring the NetScaler 9000 System

Use the console to configure the NetScaler 9000 system using its command line interface (CLI). You can access the CLI using a serial port or Telnet. If you want to use secure communications, you can access the CLI using Secure Shell (SSH).

You can also use the NetScaler 9000 system's GUI to configure the NetScaler 9000 system. The NetScaler 9000 system's GUI is a Java applet that runs within a web browser. Details about accessing the CLI and GUI are provided later in this chapter.

Figure 2-26 provides an overview of the process you will be following to configure the NetScaler 9000 system.

Figure 2-26 Overview of the NetScaler 9000 system's Configuration Process.


Login as nsroot to start configuration program
Specify the NetScaler IP Address
Specificy the netmask
Specify the default router
Specify the static routes (optional)
Specify the mapped IP address(es)
Set NetScaler timezone
Assign Administrator's (root) password
Assign NetScaler Administrator's (nsroot) password
Assign NetScaler Maintenance (nsmaint) password
Save the configuration parameters and exit the configuration program
(HA ONLY) Specify the IP of the peer node (optional)
Reeboot the NetScaler 9000 system to update network configuration
Configure the optional parameters using the CLI or GUI
Complete the post-configuration checklists

2.4.1 Initial Configuration of NetScaler 9000 System

This section describes how to configure and start a NetScaler 9000 system when it is powered-on for the first time.

Note: After you configure the parameters in this section, you can continue to configure the optional parameters as described in the section "Configuring Optional Parameters" on page 36.

1. Configuring the Ethernet Parameters

In the NetScaler 9000 systems, the Ethernet parameters are configured using the **`set interface`** CLI command.

For setting the speed/duplex mode, enter the following CLI command:

```
set interface 1/1 -speed 1000 -duplex FULL RXTX
```

where **`1/1`** is the interface for which these settings apply. Actually, those parameters cannot be set before the initial configuring is done.

Note:

Compare and confirm the interface settings with the port settings on the switch. Be aware of correct setting of flow control parameters for Gigabit Ethernet and always confirm the resulting settings after the interface came up for the first time.

To compare the interface settings with the actual port settings, use the `show interface` CLI command on the NetScaler 9x00 system. This command displays the following information:

```
> show interface

1. Interface 1/2 (NIC 0/dc0) Digital 21143-xD Fast
   Ethernet         flags=0x20c081 <ENABLED, UP,
   autoneg on, HAMONITOR ON, 802.1q support>
   mtu=1514, native vlan=1,
   eaddr=00:c0:95:c4:c7:50, uptime 52h19m43s
   Requested: media AUTO, speed AUTO, duplex AUTO,
   fctl OF
   Actual: media UTP, speed 100, duplex FULL, fctl
   OFF

 Done
```

The interface settings displayed in the `Requested` row above should match with the port settings on the switch.

2. Starting the Configuration Program

After the NetScaler 9000 system is powered-on, a login prompt is displayed on the terminal attached to the NetScaler 9000 system.

- From the command prompt, login to the `nsroot` (initial password for this account is nsroot).
- The NetScaler 9000 system's configuration program starts.

The following is displayed:

```
The NetScaler 9000 system has not been configured.

As you enter values for each configuration parameter, the
program automatically displays the next screen.

Follow the instructions in each screen.
```

Note: A value within brackets (`[]`) indicates the current value that has been set for that parameter. Empty brackets do not have a value set but will show the value after it has been set.

3. Specifying the NetScaler 9000 system's IP Address

This configuration parameter identifies the NetScaler 9000 system in the network and is used to access the system for management purposes.

Enter a unique IP address chosen for this NetScaler 9000 system when the following is displayed:

```
NetScaler 9000 system's IP Address

----------------------

This specifies the NetScaler 9000 system's IP address.

Enter the NetScaler 9000 system's IP address []:
```

4. Specifying the Netmask

This configuration parameter is the netmask for the subnet (network section) into which the NetScaler 9000 system is being installed (for example, `255.255.0.0`).

Enter the netmask when the following is displayed:

```
Netmask
-------
This specifies the netmask for the network in which the
NetScaler 9000 system is being installed.
Enter the netmask [0.0.0.0]:
```

5. Specifying Routes

In the configuration parameter, specify the IP address of the default router to which the NetScaler 9000 system sends packets.

Enter the default router's IP address when the following message is displayed:

```
Default Router IP Address
-------------------------
This specifies the IP address of the default router where
packets must be sent by the NetScaler 9000 system if the
destination IP address does not belong to the local
network.
Enter the IP address of the default router []:
```

After the default router is set, the following message is displayed:

```
Do you want to specify additional routes? [NO]:
```

- If you do not want to make any more changes to the NetScaler 9000 system's routing table, enter **NO** and then proceed to the "Specifying the NetScaler 9000 system's Mapped IP Address" on page 32.

—OR—

- Enter **YES** and proceed to next section: Adding More Routes.

◆ **Adding More Routes**

The following information is displayed.

Note: The settings in the following routing table are examples that were entered as the default router IP address parameter in the previous configuration steps.

```
STATIC ROUTES MENU

-----------------

This menu allows you to add, modify or remove entries from
the NetScaler's static routing table, which is shown
below.  Note:

- The default router must be specified.

- To apply default router changes, the system must be
rebooted.

- Each network can have only one entry in the table.

- Routes to multicast addresses are not supported.

NetScaler 9000 system ROUTING TABLE

Network     Netmask     Gateway
--------------------
default     0.0.0.0     10.101.0.1
---------------------------------------

1. Add static routes.
2. Remove static routes.
3. Remove all static routes.
4. Return to the previous menu.

Select a menu item from 1 to 4 [4]:
```

Enter **1** to display the following:

```
Add or Modify Routing Table Entries

----------------------------------

Enter the routes in the format:
'network:[netmask]:gateway', where 'network' is the IP
address of the network where traffic will be routed,
'netmask' will be applied to a destination IP address to
determine out the network address belongs to (this is an
optional value), and 'gateway' is the IP address of the
gateway where traffic will be directed.
```

```
If you enter the word 'default' as the value for
'network', then this defines the default router. Separate
route entries by a comma. For example:
default::xxx.xxx.xxx.xxx,
yyy.yyy.yyy.0:255.255.255.0:zzz.zzz.zzz.zzz

Enter the static routes to be added:
```

Next, follow these steps:

1. Enter the new route or routes according to the instructions on the screen.

   Make sure to separate each IP address by typing a colon (:) between them. Each route entry must be separated by a comma.

   For example:

   `230.10.10.1,130.40.0.0:255.255.0.0:130.40.1.1`

   After you press the <`Enter`> key, the **Static Routes Menu** is displayed.

2. Enter the number **4** to quit.
3. If you are doing initial NetScaler 9000 system configuration, proceed to "Specifying the NetScaler 9000 system's Mapped IP Address" on page 32.

- **Removing or Changing Static Routes**

  You can change, remove or add new routes to the NetScaler 9000 system's routing table.

  You can remove one, some or all of the static routes from the NetScaler 9000 system's routing table.

  To remove static routes:

  1. Go to the `STATIC ROUTES MENU`:
     - **a.** To remove one or some routes, enter **2**. Next, enter the routes to be removed. Follow the instruction displayed on the screen.

     OR

     - **b.** To remove all routes, enter **3** and follow the instructions displayed on the screen.
  2. Enter **4** to quit and return to the `STATIC ROUTES MENU.`
  3. If you are performing initial NetScaler 9000 system configuration, proceed to the next configuration step.

6. Specifying the NetScaler 9000 system's Mapped IP Address

The NetScaler 9000 system uses mapped IP addresses to establish connections between itself and the web servers connected to it.

When the client sends a request (using the web server's IP address), the NetScaler 9000 system forwards the request to the web server using the Mapped IP address specified in the Mapped IP Address parameter.

By default, the servers do not get the actual client IP address.

For the servers to get the actual client IP address, use the **`set config`** CLI command to set the client IP header information.

Note:

1. Each Mapped IP address supports up to 64,000 simultaneous TCP connections. If your web server needs more connections, you can specify additional mapped IP addresses, as described in the next section.
2. In a high availability configuration, both NetScaler 9000 systems must have the *same* mapped IP address.
3. Assigning a single mapped address may not be sufficient. If your site needs to support more concurrent connections, you can assign additional mapped IP addresses. See the section "Specifying the Netmask" on page 32.

Enter the IP address that you want to use as the mapped IP address when the following screen is displayed:

```
Mapped IP Address

-----------------

This specifies the NetScaler 9000 system's mapped IP
address that is used by the NetScaler 9000 system to
establish connections between itself and the web servers
attached to it.

Enter the mapped IP address []:
```

The NetScaler 9000 system provides a default Mapped IP address that is the next consecutive IP address after the one assigned to NetScaler 9000 system. For example, if the NetScaler 9000 system's IP address is 10.101.2.54, then 10.101.2.55 is provided as the default Mapped IP address.

7. Specifying the Netmask

This configuration parameter is the netmask for the subnet (network section) into which the NetScaler 9000 system is being installed (for example, 255.255.0.0).

Enter the netmask when the following is displayed:

```
Netmask
-------
This specifies the netmask for the network in which the
NetScaler 9000 system is being installed.
Enter the netmask [0.0.0.0]:
```

8. Specifying NetScaler Time Zone

Time Zone setting allows proper display of local time.

Note: Configuring the time zone does not change the NetScaler 9000 system's system clock.

The following is displayed:

```
Time Zone
---------
This sets the Time Zone
```

1. Press Enter to set the Time Zone
2. Press Enter key to start Time Zone setting utility.
   The Time Zone configuration utility starts.
   - Use the arrow keys to navigate the menus and the confirmation dialogs.
   - Use the <Esc> key to return to the previous menu.
3. Answer Yes to confirm that the NetScaler 9000 system's clock is set to Coordinated Universal Time (UTC).
4. Select your region from the regions list.
5. Select your country from the countries list.

a. If multiple time zones are displayed for your country, select the appropriate one.

b. Confirm the abbreviation for your local time zone.

9. Specifying the nsroot User's Password

The NetScaler system has the primary administrative user's (nsroot) password set as 'nsroot'. For security reasons, it is essential to change the default password.

The following is displayed:

```
Administrator's (nsroot) password
------------------------------
This assigns the Administrator's (nsroot) password
Changing local password for nsroot.
New password:
```

Enter new password and press Enter key. Then follow the messages to confirm the new password.

Note: If you are configuring the NetScaler 9000 system in High Availability mode, the password for the `nsroot` account must be the same on both NetScaler systems.

10. Reviewing the Parameters

Once the initial parameters are set, the menu below appears, allowing you the opportunity to review the parameters that you have set and make further changes if needed. The value that appears within the brackets ([]) indicates the currently set value for that parameter.

```
REVIEW CONFIGURATION PARAMETERS MENU
-----------------------------------
This menu allows you to view and/or modify the
NetScaler's configuration. Each configuration parameter
displays its current value within brackets if it has been
set. To change a value, enter the number that is displayed
next to it.
-----------------------------------
      1. NetScaler's IP address: [192.168.100.20]
      2. Netmask: [255.255.255.0]
      3. Default router and static routes.
      4. Mapped IP address: [192.168.100.21]
      5. Netmask for mapped IP address: [255.255.255.0]
```

```
 6. Advanced Network Configuration.
 7. Time zone.
 8. Password of the user nsroot.
 9. Cancel all the changes and exit.
10. Save all the changes and exit.
Select a menu item from 1 to 10 [10]:
```

If you need to change a parameter, select the corresponding item number in the menu and follow the instructions on the monitor or screen. The procedure is the same as described previously.

Note: Menu item 9 cancels all previously specified parameters except Time Zone and any passwords you may have modified. These changes are applied immediately in each submenu.

11. Exiting Configuration and Starting the NetScaler 9000 system

After setting values to all the items in the menu restart the NetScaler 9000 system, by selecting the item `11` in the menu and then pressing the <`Enter`> key.

The following message is displayed:

```
Writing configuration file to /nsconfig/ns.conf file
```

The system prompts a message asking the user if the user wants to reboot the NetScaler system.

All services stops and the NetScaler 9000 system reboots. The new configuration settings become effective after the reboot. The NetScaler 9000 system indicates whether the startup is successful.

When the login prompt is displayed, login to the NetScaler 9000 system by using the `nsroot` account.

Note: The NetScaler 9000 system's CLI prompt (**>**) is displayed. This interface allows you to issue any CLI command as described in the *NetScaler 9000 Series Command Reference.*

2.4.2 Configuring Optional Parameters

This section provides an overview of the optional parameters and the procedure to configure these optional parameters in NetScaler 9000 system.

1. Specifying HTTP Traffic Ports

This configuration parameter identifies the web server HTTP ports, allowing the NetScaler 9000 system to perform Request Switching for any client request that has a destination port matching to one of these configured ports.

If the incoming client request is not destined for a service or virtual server configured on the NetScaler 9000 system, the destination port in this packet must match one of the globally configured HTTP ports. This allows the NetScaler 9000 system to perform connection keep-alive/ server off-load.

To specify this optional parameter, use the `-httpPort` argument of the **`set config`** CLI command.

2. Specifying Connection Settings

You can specify the maximum number of connections made from the NetScaler 9000 system to the web server(s) attached to it. The value you enter here is applied globally to all attached servers. (For example, if you enter `500` and there are three servers attached to the NetScaler 9000 system, the NetScaler 9000 system will support a maximum of 500 connections to each of the three servers.) The default value allows an unlimited number of connections to be made.

Note: If you are using Apache Server™, you may want to set this parameter. Setting this parameter is optional for other web servers. The value set here must be equal to the value of the MaxClients parameter set in the Apache Server.

If you want to set *unique* values for one or more of the attached servers, you may do so using the **`set service`** CLI command after you complete configuring the NetScaler 9000 system.

Note: For more information, refer to NetScaler *9000 Series Command Reference* Guide.

To specify this optional parameter, use the `-maxConn` argument of the **`set config`** CLI command.

3. Enabling or Disabling Insertion of the Client's IP Address

When a web server attached to the NetScaler 9000 system receives a mapped IP address from the NetScaler 9000 system, the server identifies this mapped IP address as the client's IP address.

Some applications need the client's IP address for logging purposes or to dynamically determine the content to be served by the web server.

You can enable insertion of the actual client IP address into the HTTP header request passed from the client to one, some or all servers attached to the NetScaler 9000 system. You can then access the passed address through a minor modification to the server (via an Apache module, ISAPI interface, or NSAPI interface). NetScaler 9000 system has written sample scripts available free of charge.

Note: The global insertion of client's IP address is applicable only to pre-configured services. For all the services that are configured later, the client IP address has to be inserted manually using the **`set config`** CLI command.

To specify this optional parameter, use the `-cip` argument of the **`set config`** CLI command.

4. Setting HTTP COOKIE version

NetScaler sends its own cookie when `COOKIEINSERT` persistence is configured on a Virtual Server. It can send either HTTP COOKIE version 0 or HTTP COOKIE version 1. The default is HTTP COOKIE version 0 (mostly used on the Internet).

To specify this optional parameter, use the **`-cookieversion`** argument of the **`set config`** CLI command.

5. Setting the Maximum Requests Per Connection

For a connection between the NetScaler 9000 system and a server attached to it, you can set the maximum number of requests that the NetScaler 9000 system can pass on that connection. Setting this value to 0 allows an unlimited number of requests to be passed.

To specify this optional parameter, use the -maxReq argument of the **set config** CLI command.

2.4.2.1 Configuration Procedure for Optional Parameters (Using the CLI)

To configure these optional parameters using the CLI, proceed as follows:

1. Use the **set config** command at the CLI command prompt.

   Example:

   ```
   set config -httpPort 80 -cip ENABLE clientIP -maxReq
   1000 -maxConn 500 –cookieversion 0
   ```

2. Save your changes by entering the **save config** command at the **>** CLI command prompt.

   The **show config** CLI command displays all the settings that have been configured with the **set config** CLI command.

Note: For more information on the reboot procedure, refer to "Restarting the NetScaler 9000 system" on page 43.

2.4.3 Post-Configuration Checklists

Complete the following checklists after you finish the NetScaler 9000 system configuration:

NetScaler 9000 system CONFIGURATION CHECKLIST
The build suggested by NetScaler 9000 system staff is running. NetScaler 9000 system Build Number: _____
If upgrading from a previous build, there are no incompatibility issues. (Incompatibility issues are documented in the build's release notes.)

The NetScaler 9000 system port settings are the same as the switch's port settings: The port(s) settings are (speed, duplex, flow control, monitoring):

_____

_____

_____

Enough mapped IP addresses have been configured to support all the server-side connections during peak times.

- The number of configured mapped IP addresses are: ____
- The expected number of simultaneous server connections is:

  [ ] 62,000 [ ] 124,000 [ ] Other

TOPOLOGY CONFIGURATION CHECKLIST
The NetScaler 9000 system's **`add route`** CLI command has been used to resolve servers on other subnets (see the "Multiple Subnets" section in this chapter): The **`add route`** command(s) entered were: _____ _____ _____
If the NetScaler 9000 system will be in a public-private topology (see the "Multiple Subnets" section in this chapter), reverse NAT has been configured on the NetScaler 9000 system. The **`add route`** command(s) entered were:_____ _____ _____ _____
The fail over (high availability) settings configured on the NetScaler 9000 system resolve in a one arm or two-arm configuration. ALL unused network interfaces have been disabled: _____ _____

	If the NetScaler 9000 system is placed behind an external load balancer, then the load balancing policy on the external load balancer is not “least connection.” The load balancing policy configured on the external load balancer is: _____
	If the NetScaler 9000 system is placed in front of a firewall, then the session time-out on the firewall is set to a high value (greater than or equal to 300 seconds). The value configured for the session time-out is: _____

SERVER CONFIGURATION CHECKLIST	
	“Keep-alive” has been enabled on all the servers. The value configured for the keep-alive time-out is: _____
	The default gateway has been set to the correct value (the default gateway should either be the NetScaler 9000 system or upstream router. The default gateway is: _____
	Are the servers’ port settings are the same as the switch’s port settings? The port(s) settings are (speed, duplex, flow control, monitoring): _____ _____ _____
	If the Microsoft® Internet Information Server will be used, buffering has been enabled on the server.

If the Apache Server will be used, the MaxConn (maximum number of connections) parameter has been configured on the server and on the NetScaler 9000 system.

The MaxConn (maximum number of connections) value that has been set is:

_____

If the NetScape® Enterprise Server™ will be used, the maximum requests per connection parameter is set on the NetScaler 9000 system.

The maximum requests per connection value that has been set is:

_____

SOFTWARE FEATURES CONFIGURATION CHECKLIST

Does the NetScaler 9000 system's layer 2 mode feature need to be disabled? (Disable if another layer 2 device is working in parallel with the NetScaler 9000 system.)

Reason for enabling or disabling:

_____

_____

Does the NetScaler 9000 system's MAC-based forwarding feature need to be disabled?

(If the MAC address used by return traffic is different.)

Reason for enabling or disabling:

_____

_____

Does host-based reuse need to be disabled?

(Is there virtual hosting on the servers?)

Reason for enabling or disabling:

_____

_____

Do the default settings of the NetScaler 9000 system's surge protection feature need to be changed?

Reason for changing or not changing:

_____

_____

ACCESS CHECKLIST

- The NetScaler 9000 system IPs can be pinged from the client-side network.
- The NetScaler 9000 system IPs can be pinged from the server-side network.
- The server(s) can be pinged through the NetScaler 9000 system.
- Internet hosts can be pinged from the servers.
- The server(s) can be accessed through the browser.
- The Internet can be accessed from server(s) using the browser.
- The NetScaler 9000 system can be accessed from SSH and Telnet.
- The admin access to the server(s) is working.

Note: When you are using the PING utility, ensure that the pinged object (server…) has the ICMP ECHO enabled else your PING will not succeed.

FIREWALL CHECKLIST

These firewall requirements have been met:

- UDP 161 (SNMP)
- UDP 162 (SNMP trap)
- TCP/UDP 3010 (NetScaler 9000 system GUI)
- HTTP 80 (NetScaler 9000 system GUI)
- TCP 22 (SSH)
- TCP 23 (Telnet)

2.5 Maintaining the NetScaler 9000 System

After initial configuration, the following are the procedures that you need to perform for maintaining the NetScaler 9000 system:

- Reconfiguring the NetScaler 9000 system
- Restarting the NetScaler 9000 system
- Powering-Off the NetScaler 9000 system

2.5.1 Reconfiguring the NetScaler 9000 system

If you want to review and/or change the NetScaler 9000 system's configuration menu settings, enter the following command at the CLI command prompt:

```
config ns
```

The NetScaler 9000 system's configuration program starts running. Use the Configuration menu to change or reconfigure the NetScaler 9000 system settings.

2.5.2 Restarting the NetScaler 9000 system

To restart the NetScaler 9000 system, follow these steps:

1. To reboot the NetScaler 9000 system, enter the following CLI command:

   ```
   > reboot ns
   ```

2. The **LOGIN** prompt appears. Use a valid Login name and password to connect to the NetScaler 9000 system.

   The CLI prompt (**>**) is displayed.

2.5.3 Powering-Off the NetScaler 9000 system

If you need to power-off the NetScaler 9000 system, **ensure** that you do it as follows:

- **From CLI prompt**

  At the CLI prompt, enter the following command:

  ```
  > shutdown
  ```

  A series of messages are displayed on the terminal screen indicating that the NetScaler 9000 system has been halted

- **In the NetScaler 9400 model**

  Press the **ON/OFF** switch on the backside of the system once. The green LED above the switch is turned off.

  Note: For more information, refer to Figure 2-22 for the switch's location.

- **In NetScaler 9800-T or NetScaler 9800-SX models**

  Press the **ON/OFF** switch on the backside of the system and HOLD IT DOWN for four seconds.

  Note: For more information, refer to Figure 2-25 for the switch's location.

At any time after you have powered off the NetScaler 9000 system, you can restart it by depressing the **ON/OFF** switch once. The green LED above the switch will illuminate.

2.6 Managing the NetScaler 9000 System

This section describes how to manage the NetScaler 9000 system, including:

- Accessing the Command Line Interface (CLI)

- Accessing the Graphical User Interface (GUI)
- SNMP Support
- System Users and Groups
- Resetting the nsroot User Password

2.6.1 Accessing the Command Line Interface (CLI)

You can access the NetScaler 9000 system's CLI using any of the following methods:

- Serial port
- Secure Shell (SSH)
- Telnet or FTP

Note: For information about the features of the CLI, see the *NetScaler 9000 Series Command Reference*.

2.6.1.1 Serial Port

Connect the serial port of the NetScaler 9000 system to your PC serial port and start the Hyper Terminal program (or any other terminal emulation program you prefer). The NetScaler 9000 system Login prompt appears (if it is not then press ENTER for few times). Login to NetScaler 9000 system using your *Username* and *Password*.

The CLI prompt **`'>'`** is displayed on the monitor.

2.6.1.2 Secure Shell (SSH)

The SSH protocol is the preferred remote access method for accessing the NetScaler system. You can connect remotely to the CLI using an SSH client.

1. Download and install one of these SSH clients (tested and supported by NetScaler 9000 system):

- "SecureCRT 3.4" (Windows platform)
  Available at site:
  `http://tucows.com/preview/194267.html`
- "F-Secure SSH Client 5.2" (Windows platform)
  Available at site:
  `http://www.f-secure.com/download-purchase/`

- "putty.exe"
  Available at site:
  `http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`

2. Open a new session on the client by specifying the following:

- NetScaler 9000 system's IP address as the host name
- Protocol version (either version of ssh 1 or ssh 2 can be used to connect to the NetScaler 9000 system)
- *Username* (**`nsroot`**) and the password for the NetScaler 9000 system

The following text shows a session conducted through SSH access.

```
login: nsroot
Password:
Last login: Mon Sep 27 10:03:45 from 10.100.3.26
 Done
>
```

2.6.1.3 Other Access Methods

If you wish to access the NetScaler command line interface via telnet or you require FTP access to the system, you must enable these protocols as they are disabled by default for security reasons. To enable these protocols, follow these steps.

1. Log into the system through the serial console as the nsroot user.

2. Run the '`shell`' command. The system prompt will change from '>' to '#' indicating that you are now running in the system shell.

3. Copy the /etc/inetd.conf file to /nsconfig/inetd.conf.

```
> cp /etc/inetd.conf /nsconfig/inetd.conf
```

4. Open the /nsconfig/inetd.conf file and uncomment the '#' symbol at the beginning of the configuration line for the protocol you wish to enable. Then save the file.

5. Reboot the NetScaler system to activate the change with the 'reboot ns' command.

2.6.2 Accessing the Graphical User Interface (GUI)

You can configure the NetScaler 9000 system by running and using NetScaler 9000 system's GUI configuration program, which is a web-based applet.

The NetScaler 9000 system GUI applet requires that you have version 1.3.1_01 of the Java® applet plug-in. The subsection "About the Required Java Plug-In" provides information about the plug-in and its installation.

2.6.2.1 System Requirements

The system requirements for the computer on which the GUI will be running are as follows:

Windows

Pentium® 166 MHz or faster processor with at least 48 MB of RAM is recommended for applets running in a browser using a Java plug-in product. You should have 40 MB free disk space before installing the plug-in.

Linux

A Pentium platform running Linux kernel v2.2.12 and glibc version 2.12-11 or later. A minimum of 32 MB RAM is required. Recommended 48 MB RAM, 16-bit color mode, KDE and KWM window managers used in conjunction with displays set to local hosts.

Solaris

The Java 2 Runtime Environment, Standard Edition, version 1.3.1_01 is intended for use on Solaris 2.6, Solaris 7 and Solaris 8 operating environments.

Prior to installing the Java 2 Runtime Environment, ensure that you have installed the full set of required patches needed for support of this release.

See the "Solaris Patch Installation" section before proceeding. See also "Solaris Font Package Requirements" section for information about which font packages should be on your system.

2.6.2.2 About the Required Java Plug-In

You can install the plug-in by accessing one of these resources:

- NetScaler 9000 system GUI applet - see the subsection “Installing the Java Plug-In from the GUI.”
- NetScaler 9000 system web site - see the subsection “Installing the Java Plug-In from NetScaler 9000 system’s Web Site.”

Note: If either of the above methods does not work, you can install the plug-in another way (see the “Installing the Java Plug-In When You Cannot Install It from the GUI or NetScaler 9000 system Web Site” subsection).

The following web browsers/platforms have been tested and can be used for the installation:

- Internet Explorer version 4, 5, or 5.5 on Windows 95/98/2000/NT
- Internet Explorer version 6 on Windows XP Home or Professional editions
- Netscape 4.51/4.61/4.72/4.75 on Windows 95/98/2000/NT
- Netscape 4.51 on Solaris 5.6/5.7/5.8
- Netscape 4.61/4.72/4.75 on “Red Hat Linux 6.2”
- Netscape 4.77 on Windows 2000/NT, or on Windows XP Home or Professional editions
- Netscape 6.2 on Windows 98/2000/NT, or on Windows XP Home or Professional editions

2.6.2.3 Installing the Java Plug-In from the GUI

Proceed as follows:

1. Access the GUI from your web browser:
   a. Type the URL in the following format:

      http://*IP_address_of_NetScaler 9000 system*

WARNING! If there are two NetScaler 9000 systems in a high availability (fail over) setup, make sure that you do not access the GUI by entering the IP address of the secondary NetScaler 9000 system. If you do this and use the GUI to configure the

secondary NetScaler 9000 system, any configuration change is not applied to the primary NetScaler 9000 system.

b. Press the <Enter> key.

2. When the NetScaler 9000 system applet's main window is displayed, click on the "**NetScaler Configuration Utility**" link.

Note: If you are running the applet for the first time, the following window is displayed else skip to step 5.

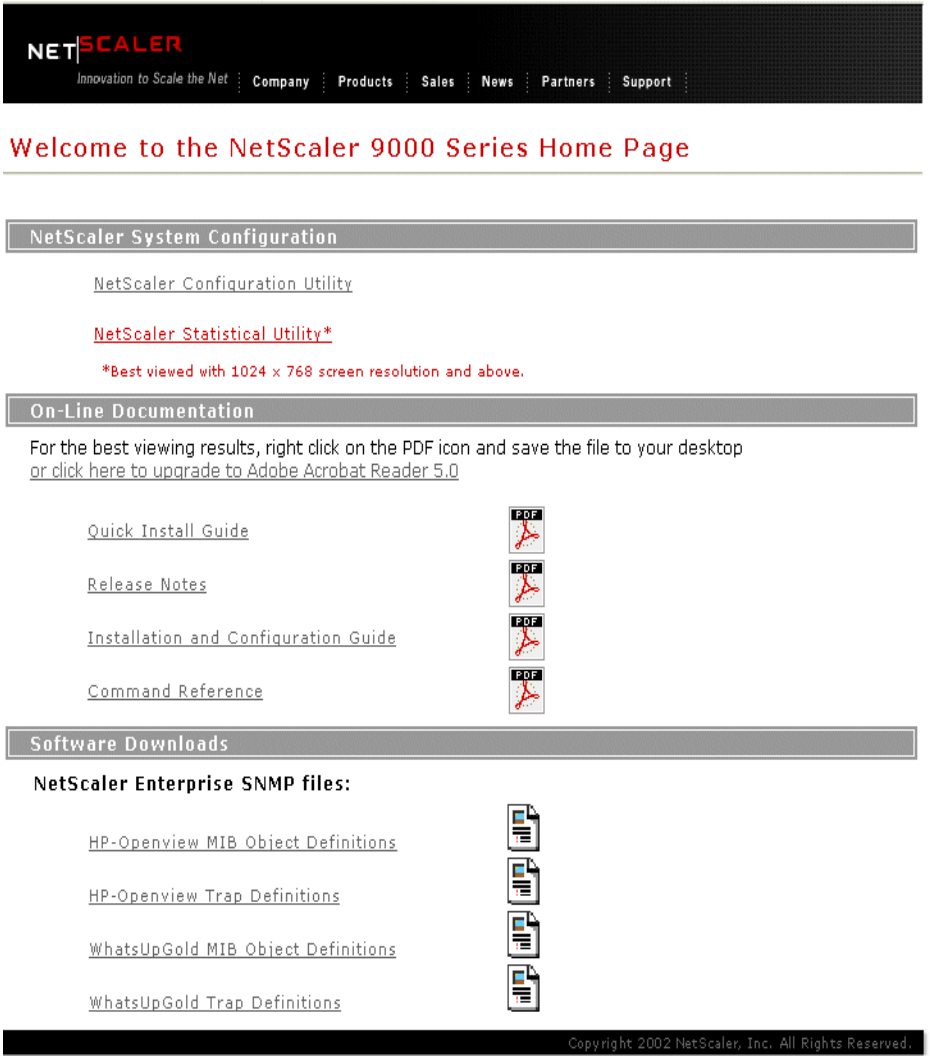
Figure 2-27 Download Java2 Runtime dialog

Security Warning
Do you want to install and run "Java 2 Runtime Envrionment" signed on 8/8/2001 3:03 PM and distributed by:
Sun Microsystems, Inc.
Publisher authenticity verified by VeriSign Commercial Software Publishers CA
Caution: Sun Microsystems, Inc. asserts that this content is safe. You should only install/view this content if you trust Sun Microsystems, Inc. to make that assertion.
Always trust content from Sun Microsystems, Inc.
Yes
No
More Info

3. Download the Java plug-in according to the screen instructions.

4. After the download is complete, the following window is displayed:

Figure 2-28 NetScaler 9000 Series Home Page.

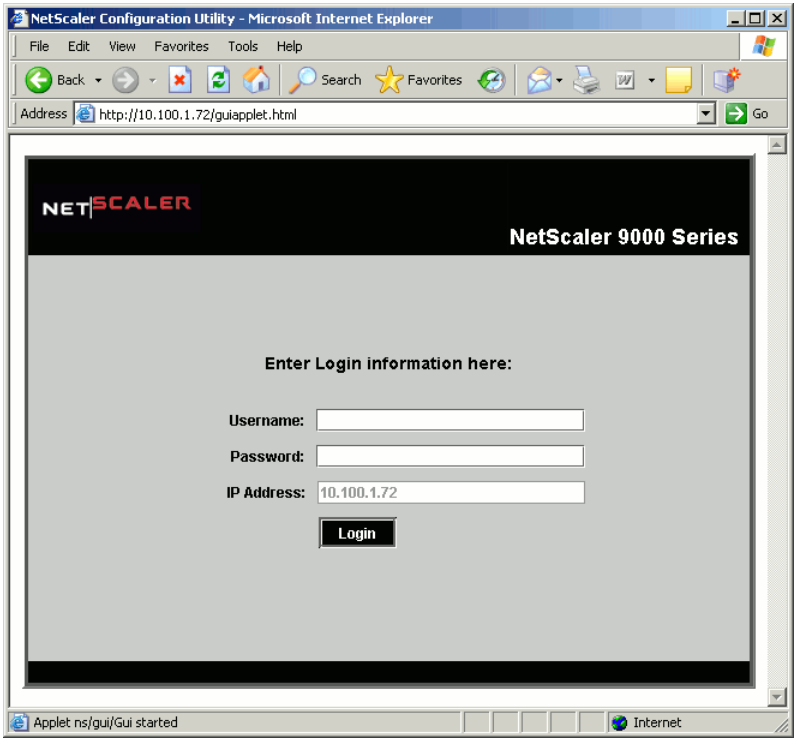

NETSCALER
Innovation to Scale the Net
Company
Products
Sales
News
Partners
Support
Welcome to the NetScaler 9000 Series Home Page
NetScaler System Configuration
NetScaler Configuration Utility
NetScaler Statistical Utility*
*Best viewed with 1024 x 768 screen resolution and above.
On-Line Documentation
For the best viewing results, right click on the PDF icon and save the file to your desktop
or click here to upgrade to Adobe Acrobat Reader 5.0
Quick Install Guide
Release Notes
Installation and Configuration Guide
Command Reference
Software Downloads
NetScaler Enterprise SNMP files:
HP-Openview MIB Object Definitions
HP-Openview Trap Definitions
WhatsUpGold MIB Object Definitions
WhatsUpGold Trap Definitions
Copyright 2002 NetScaler, Inc. All Rights Reserved.

5. The NetScaler Home page enables you to access the following utilities:

- Click the “NetScaler Configuration Utility” hyperlink to access the NetScaler 9000 system’s GUI.
- Click “NetScaler Statistical Utility” hyperlink, to access the NetScaler’s Graphical Dashboard. For more information on using the NetScaler’s Graphical Dashboard, see Chapter 4, “NetScaler Statistical Utility”.

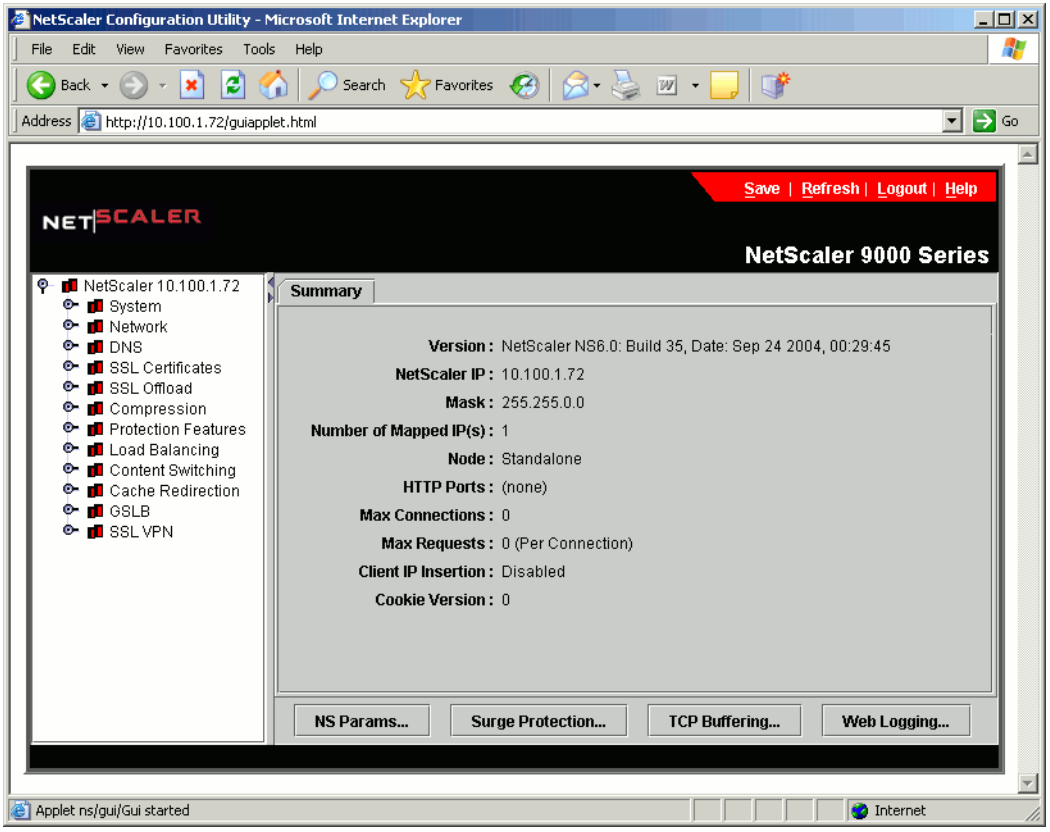
When you click the “NetScaler Configuration Utility” hyperlink, the following window is displayed:

Figure 2-29 NetScaler Login Window



6. Type the *Username* and *Password* for a system user, such as the nsroot user. Click the Login button.
7. The following NetScaler 9000 system applet screen is displayed in your browser

Figure 2-30 NetScaler 9000 System GUI



8. If you need to access the NetScaler 9000 system applet's documentation, select Help Topics from the NetScaler 9000 system applet's Help menu at the top right corner.

   The main help screen is displayed in your browser.

2.6.2.4 Installing the Java Plug-In from NetScaler's Web Site

To download the plug-in directly from the NetScaler's web site, proceed as follows:

1. In your web browser, type the following URL: http://www.netscaler.com
2. Click the **Support** button on the web page.
3. Click the **Download-Java** link.

4. Follow the installation instructions to download java plug-in from the NetScaler's web site.
5. After downloading the Java applet, type the following URL in your browser:

   http://*IP address of your NetScaler 9000 system*

   where *`IP address of your NetScaler 9000 system`* is the actual IP address of the NetScaler 9000 system on which the GUI applet resides.

   The Login window is displayed. Proceed with steps 4 - 7 as mentioned in the "Installing the Java Plug-In from the GUI" on page 48.
6. After the download, the **Login** window is displayed.
7. Type the *Username* and *Password* that allow NetScaler 9000 system access and then click the **Login** button.
8. The NetScaler 9000 system GUI screen is displayed in your browser. Refer to Figure 2-30 on page 52.

Note: If you need to access the NetScaler 9000 system applet's documentation, select help topics from the **Help** menu from the top right corner of the GUI.

2.6.2.5 Other methods to Install Java Plug-In

If you are using a Netscape or other type of web browser and you cannot successfully download from the NetScaler 9000 system web site or by accessing the GUI applet, install the plug-in as follows:

1. In your web browser, enter the URL and port number of your NetScaler 9000 system:

   http://*IP_address_of_NetScaler 9000 system***:80**

   where *`IP_address_of_NetScaler 9000 system`* is the NetScaler 9000 system's IP address.

Note: If there are two NetScaler 9000 systems in a high availability (fail over) setup, make sure that you do not access the GUI by entering the IP address of the secondary NetScaler 9000 system. If you do this and use the GUI to configure the secondary NetScaler 9000 system, any

configuration change is not applied to the primary NetScaler 9000 system.

2. Click on the plug-in icon that is displayed and then follow the screen instructions.

   This places the Java plug-in setup icon (for example, "j2re-1_3_1_01-win") on your computer at the location you specified.

3. Double click the plug-in setup icon and follow the installation instructions.

4. Afterwards, return to the web browser, and then click the plug-in icon to display the GUI login window.

2.6.3 SNMP Support

When you configure SNMP support in the NetScaler 9000 system, you can use CLI commands to do the following:

- Assign access privileges to network management applications and their users
- Specify NetScaler 9000 system information that can be displayed from the NetScaler 9000 system's MIB
- Specify SNMP traps that notify you if the NetScaler 9000 system's CPU usage becomes a concern, if NetScaler 9000 system interfaces or connections to the servers are disconnected or reconnected, and/or if fail over has occurred, and whenever the syn flood count has reached the configured threshold.

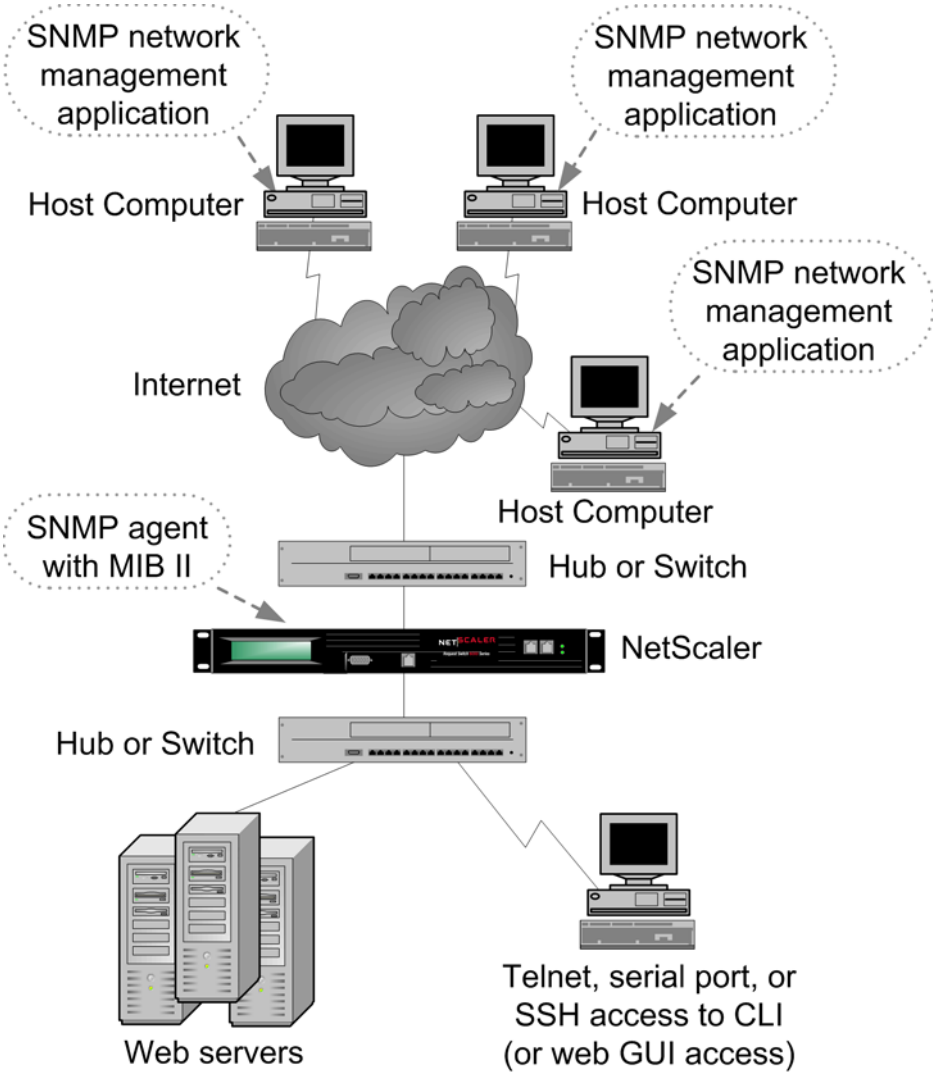
Figure 2-31 shows the SNMP configuration: The network management application uses SNMP versions 1 or 2 to communicate with the SNMP agent on the NetScaler 9000 system. The agent communicates with the MIB to collect data requested by the application. Figure 2-11 shows the NetScaler 9000 system in the SNMP environment. The NetScaler 9000 system supports a subset of the groups in MIB II. NetScaler 9000 system supports an enterprise-specific MIB.

The NetScaler 9000 system supports enterprise -specific MIBs. They are:

- A subset of standard MIB-2 groups: `SYSTEM, IF, ICMP, UDP, SNMP.`

- A NetScaler 9000 system enterprise MIB: providing the NetScaler 9000 system specific configuration and statistics.

Figure 2-31 NetScaler 9000 system Supporting SNMP



2.6.3.1 Bilingual Network-Management System

The SNMP agent on the NetScaler system supports both SNMPv1 and SNMPv2. As a result, the agent works in a bilingual mode. This implies that, an agent can handle SNMP version 2 queries, including Get-Bulk. It also

sends out traps compliant with SNMPv2, and supports the SNMPv2 data-types like counter64.

V1 managers use the NS-MIB-smiv1.mib file and V2 managers should use the NS-MIB-smiv2.mib file.

2.6.3.2 Configuring SNMP on the NetScaler 9000 system

The configuration process consists of these tasks:

- Set the access control list for SNMP managers.
- Set the SNMP community, which defines the access privileges (Read operation).
- Set the NetScaler's system MIB variables (system name, contact person for that system and system location).
- Set which traps will be enabled and where the trap notification will be displayed.
- Set the threshold level for the all traps, which causes an alarm to occur. This event generates a notification message to an SNMP network management application if the threshold level has been reached.
- (Optional) The SNMP service runs on the NetScaler 9000 system IP address. You can change the NetScaler 9000 system IP address to another IP address.

Proceed as follows (for additional details on the CLI commands, see the *NetScaler 9000 Series Command Reference*):

1. Set access privileges for the network management application by entering the following CLI command:

   `add snmp manager <`*`IPAddress`*`> . . [-netmask <netmask>]`

   where *`IPAddress`* is the IP address of the client host computer on which the network management application resides. A maximum of 10 managers (IP addresses) can be specified.

   - If you do not add a manager, SNMP queries from *all* managers will be processed.
   - If you add one or more managers, the SNMP queries *only* from these managers will be processed.

   After you have defined the access control list for the network management application; you may choose to:

- Delete access privileges for a network management application using the **`rm snmp manager`** CLI command.
- Display which network management applications have access privileges using the **`show snmp manager`** CLI command. The IP addresses of these applications are displayed on the screen.

2. Set access privileges for the user of the network management application by entering the following CLI command:

`add snmp community <`*`communityName`*`> <`*`permissions`*`>`

where *`communityName`* is the name of the community to which the user belongs and *`permissions`* is the task that a user can perform. The *`permissions`* argument can be set as `GET, GET_NEXT, GET_BULK,` or `ALL`.

Note: For more information, refer to NetScaler *9000 Series Command Reference.*

A maximum of 20 communities can be added. The community name can be a maximum of 32 characters.

After the user privileges have been set, if you need to:

- Delete a user's access privileges. Use the **`rm snmp community`** <*`communityName`*> CLI command.
- Display which users have access privileges. Use the **`show snmp community`** CLI command.

3. Set the NetScaler's system variables in the MIB by entering the following CLI command.

`set snmp mib -contact <`*`sysContact`*`>`
`-name <`*`sysName`*`> -location <`*`sysLocation`*`>`

where *`sysContact`* provides contact information for the person(s) in your organization responsible for the NetScaler 9000 system, *`sysName`* is the name you give to the NetScaler 9000 system, and *`sysLocation`* identifies the NetScaler 9000 system location.

A maximum of 128 characters can be entered for each of these arguments.

After you have set the NetScaler 9000 system's system variables in the MIB, if you need to:

- Change these MIB settings, use the same CLI command.

- Display what has been set. Use the **`show snmp mib`** CLI command. The settings are displayed on the screen.

4. Set the SNMP traps by entering the following CLI command:

   `add snmp trap (GENERIC | SPECIFIC) <trapDestination>..[-version ( V1 | V2 )]`

   where in the:

   - **`(GENERIC | SPECIFIC)`**: select an option to set the trap type as generic or specific.
   - **`<trapDestination>`**: specify the IP address of the client where the traps need to be displayed.

   SNMP traps are asynchronous events generated by the agent to indicate state of the system.

   The destination to which these traps should be sent needs to be configured. This specifies the system to which the traps have to be sent.

   A maximum of 10 IP addresses (enterprise-specific trap destinations) can be entered. A maximum of five IP addresses (generic trap destinations) can be entered.

Note: If more than 10 authentication traps are generated within 20 seconds, no traps will be generated for the next 60 seconds.

NetScaler supports three generic (specified in RFC1213) traps and seven enterprise specific traps.

A maximum of five destinations can be configured for generic traps and 10 for enterprise specific traps.

Generic Trap

For example, to generate a *generic* trap enter the following CLI command:

`add snmp trap generic 10.102.1.1`

In this example, the NetScaler 9000 system is set to display generic trap notice on 10.102.1.1 as listed in the table below:

The NetScaler 9000 system can be set to notify the following *generic* traps

Table 2-2 : Table describing Generic Traps and description

Generic trap Name	Description
`authenticationFailure`	A notification is displayed when a SNMP management application attempts to access the NetScaler 9000 system and this application does not have access privileges.

Specific Traps

For example, to generate a *specific* trap enter the following CLI command:

```
add snmp trap specific 10.102.1.1
```

In this example, the NetScaler 9000 system is set to display a notice on 10.102.1.1 when the CPU utilization on the system exceeds a predefined threshold.

Table 2-3 The NetScaler 9000 system can be set to notify following *specific* traps:

Specific trap Name	Description
`changeToPrimary`	A notification is displayed when the NetScaler 9000 system is in a high availability configuration becomes the primary - active NetScaler 9000 system.
`changeToSecondary`	A notification is displayed when the NetScaler 9000 system is in a high availability configuration becomes the secondary - passive NetScaler 9000 system.
`cpuUtilization`	A notification is displayed when the CPU utilization exceeds the predefined threshold.
`cpuUtilizationNormal`	This trap indicates that the CPU utilization has returned to normal.
`entityup`	This trap is sent when the state of the interface, vserver, or physical service changes to UP.

Specific trap Name	Description
entitydown	This trap is sent when the state of the interface, vserver, or physical service changes to DOWN.
synflood	A notification is displayed when the rate at which unacknowledged syns received exceeds the threshold value.
synfloodNormal	This trap is sent when the rate at which, unacknowledged SYN packets are received, returns to normal.
memoryUtilization	This trap is sent when the utilization of memory exceeds the threshold value.
memoryUtilizationNormal	This trap is sent when the utilization of memory returns to normal.
vServerRequestRate	This trap is sent when the request rate on a vserver exceeds a threshold value.
vServerRequestRateNormal	This trap is sent when the request rate on a vserver returns to normal
serviceRequestRate	This trap is sent when the request rate on a service exceeds a threshold value.
serviceRequestRateNormal	This trap is sent when the request rate on a service returns to normal.
entityRxRate	This trap is sent when the request bytes of a vserver/service exceeds a threshold value.
entityRxRateNormal	This trap is sent when the request bytes of a vserver/service returns to normal.
entityTxRate	This trap is sent when the response bytes of a vserver/service exceeds a threshold value.
entityTxRateNormal	This trap is sent when the response bytes of a vserver/service returns to normal.

Specific trap Name	Description
entitySynflood	This trap is sent when the number of unacknowledged SYN packets for a vserver/service exceeds a threshold value.
entitySynfloodNormal	This trap is sent when the number of unacknowledged SYN packets for a vserver/service returns to normal.

Note: The eighth enterprise specific trap for `syn_flood` is also available.

Remove Traps

To stop trap notice(s) from being sent to server(s) enter the following CLI command:

```
rm trap (generic | specific) <trapDestination>...
```

where

- **(generic | specific)** is the trap type.
- **<trapDestination>** is the IP address of the client that will not receive trap message(s).

View Traps

To view the traps enabled on the NetScaler 9000 system and the list of clients receiving the trap notice(s), enter the following CLI command:

```
show trap
```

The trap type and the corresponding client IP addresses are displayed on the screen.

5. Set the threshold for traps by entering the following CLI command:

```
set snmp alarm <trapName> <thresholdValue>
[-normalValue <positive_integer>] [-time
<secs>][-state ( ENABLED | DISABLED )]
```

Where <trapName> = (CPU | MEMORY | SYNFLOOD | VSERVER-REQRATE | SERVICE-REQRATE | ENTITY-RXRATE | ENTITY-TXRATE | ENTITY-SYNFLOOD)

After the relevant threshold levels have been set, you can display them at any time by using the **`show snmp alarm`** command. When these threshold levels are breached, SNMP traps are sent to the destinations specified by the `add snmp trap` command

6. (Optional) Enable SNMP access on other IP addresses.

   `set ns ip <IPAddress> -snmp ENABLED -mgmtAccess ENABLED`

   Where IPAddress is any NetScaler owned IP address.

2.6.3.3 Importing SNMP MIB Files to the SNMP Manager on the Host Computer

Proceed as follows:

- If the **HP OpenView** SNMP manager is on your host computer, copy the `NS-MIB-smiv2.mib` file from the /Utilities/`SNMP/HP_OpenView` directory in the NetScaler 9000 system product CD or download it from the FTP site: upload.netscaler.com.
- If the **WhatsUpGold** SNMP manager is on your host computer, copy the `traps.txt` and `mib.txt` files from the /Utilities/`SNMP/WhatsUpGold` directory in the NetScaler 9000 system product CD or download it from the FTP site: upload.netscaler.com.

Note: For more information on the *Username* and *Password* used to connect to the FTP site, contact the NetScaler 9000 system product support group.

2.6.4 System Users and Groups

All NetScaler systems are configured with the default nsroot user. The list here details important characteristics of the nsroot user.

- The nsroot user is immutable and always has full system privileges.
- The nsroot user is not subject to any policy which is configured on the system. This means that command and authentication polices cannot be used to modify the nsroot user's access to the NetScaler system.
- The nsroot user cannot be bound in to group memberships.

- The nsroot user's default password is nsroot. It is strongly advised that you change your NetScaler's nsroot password immediately on powering it up for the first time.

In addition to the nsroot user, the NetScaler system allows you to create system users and groups to organize these users in to. The remainder of section 2.6.4 discusses managing these users and groups. Before proceeding on, it is important to first explain the system global scope. System global is the entity representation for the system level scope. This entity is available for the purpose of setting NetScaler system level parameters and policies. Excluding nsroot, all of the NetScaler system users and groups are affected by system global applied policies and parameters.

2.6.4.1 Creating System Users and Groups

To create users and groups, you will use the add action. The example here shows this usage. The first string after `user` is the desired username and the string following that is the user's password.

```
> add system user johnd johnd4689
```

When you enter the password as shown here it will be displayed in clear text. However, system user passwords are stored on the NetScaler in an encrypted format.

To create a system group you will use a similar add action.

```
> add system group nocusers
```

To add system users to system groups, you will use the bind action as illustrated here.

```
> bind system group nocusers -username johnd
```

It is allowable to bind users into more than one group. Binding your system users into multiple groups will allow more flexibility when applying command policies, which are discussed a bit later in this chapter. Once system users and groups are created, you can view details about them with the show action.

```
> show system users
        2 Configured system users:
1)      User name: nsroot
2)      User name: johnd
```

```
 Done
> show system group
        1 Configured system group:
1)      Group name: nocusers
 Done
```

To view further detail about group membership, use the show action directly against the user or group in question.

```
> show system user johnd
User name: johnd
Group name: nocusers
Done
> show system group nocusers
        Group name: nocusers
        User name: johnd
 Done
```

The resulting output will list all of the groups to which a user belongs or which users are members of the group which you specify.

2.6.4.2 Changing System User Passwords

Should the need arise to change system user passwords you will use the `set` action as shown here. Note once again that the password you enter will be shown in the nscli as clear text but will be stored internally in an encrypted format.

```
> set system user johnd newpasswd1
```

When resetting the nsroot user's password, you will use this command as well. If you've lost the nsroot user's password, you can recover it with the procedure discussed in the "Resetting the nsroot User Password"section later in this chapter.

2.6.4.3 Removing System Users and Groups

When removing users or groups you will use the `rm` action. Before you can successfully remove users or groups however, you must first unbind all relevant group memberships before the system will let the removal proceed.

```
> unbind system group nocusers -username johnd
 Done
> rm system user johnd
 Done
> show system users
        1 Configured system user:
1)      User name: nsroot
 Done
> show system group
        1 Configured system group:
1)      Group name: nocusers
 Done
> rm system group nocusers
 Done
```

2.6.4.4 Resetting the nsroot User Password

In order to reset your root password, you must boot the NetScaler system in to single user mode, mount the file systems in read/write mode, and remove the 'set system user nsroot' entry from the ns.conf file. This process does not recover your root password, but will allow you to reset it to the default setting of 'nsroot' and then enter a new password.

- **To recover the password**

1. Accessing the NetScaler system via the serial console, boot in single user mode.

   As the operating system starts, it displays the following message:

```
Hit [Enter] to boot immediately, or any other key for command prompt.
```

```
Booting [kernel] in 9 seconds...
```

2. Press the space bar immediately and the following message is displayed:

```
Type '?' for a list of commands, 'help' for more detailed help.
ok
```

3. Enter the command '**`boot -s`**' and then press the <Enter> key to start the NetScaler system in single user mode.

   After the system boots, the following message is displayed:

```
Enter full pathname of shell or RETURN for /bin/sh:
```

4. Press the <Enter> key to display the # prompt.
5. Enter the following command at the shell prompt to mount the file systems:

   `mount /dev/dev/ad0s1a /flash`

6. Edit the /flash/nsconfig/ns.conf file, removing the 'set system user nsroot" entry. Save the file and exit.
7. Reboot the system with the '`reboot`' command.
8. When the system completes rebooting login as 'nsroot' with the password 'nsroot'.
9. Once logged in to the system you will be forced to enter a new 'nsroot' user password. Once you finish, exit the config ns menu with option

2.6.4.5 Using Roles Based Authorization Command Policies

Where the system users and groups functions allows administrators to define *who* has access to the NetScaler system, Roles Based Authorization (RBA) allows definition as to *what* systems users and groups are permitted to access on the NetScaler system. To create these definitions, administrators use command policies to regulate what commands, command groups, vservers, or any other NetScaler element system users and groups are permitted to use. Here are the key points to keep in mind when using command policies.

- The NetScaler 9000 system has a fixed default DENY system command policy. In practice, this has several effects.
- There can be no globally bound system command authorization policy. Command policies can be bound directly to system users and groups only.
- Users or groups with no associated command policies are subject to the default DENY command policy and will therefore not be able to execute any commands until policies are expressly bound to them.

- Command policy inheritance - All users inherit the policies of the groups to which they belong.
- Explicit policy prioritization - Priorities must be assigned to all policies when bound to users and groups to define precedence in policy enforcement by the system against user actions.

2.6.4.6 Creating Command Policies

The syntax for creating a command policy uses a basic add action, as shown below. With the add action, you will define either an ALLOW or DENY policy action which is based on a command specification expression. This expression enumerates an area of command line usage, which the policy will allow or deny user access to once it is bound. The command example below illustrates this complete structure.

```
add system cmdPolicy <policyName> (ALLOW|DENY) <cmdSpec>
```

To build a command policy, standard regular expressions are used for the `cmdSpec` parameter to match commands on the NetScaler Command Line Interface. Before creating these regular expressions for command policies, keep these following points in mind.

- Command policy regular expression strings must be enclosed in double quotes when added.
- Command policy regular expressions are case insensitive.
- The 'help' command is not subject to any command policies.

The table below illustrates a few sample cmdSpec regular expressions and what commands they will match.

Command Specification	Matches These Command Attempts
"^rm.*"	All remove actions
"^show.*"	All show commands
"^shell"	The shell command
"^add\s+vserver.*"	Create a vserver
"^add\s+(lb\s+vserver).*"	Create an lb vserver
"^set\s+lb.*"	Set load balancing settings at the command group level

The next set of examples puts these sample command specifications in to use in full command policies.

```
> add system cmdPolicy deny_all_rm DENY "^rm.*"
= Prevents all removal actions
> add system cmdPolicy deny_all_sh DENY "^shell"
= Prevents access to the shell.
> add system cmdPolicy allow_shows ALLOW "^show.*"
= Allows show actions
> add system cmdPolicy allow_vserver ALLOW
"^add\s+vserver.*"
= Policy to allow creation of vservers.
> add system cmdPolicy deny_system_cmnd DENY "*.system.*"
= Prevents modification of system command group level
settings (including command policies)
> add system cmdPolicy default_deny_override ALLOW "^.*"
= Policy to override the system default DENY command
policy and allow full command access.
```

Note: Regular expression support is offered for those users with the resources to maintain more customized expressions and those deployments that require the flexibility regular expressions offer. For most users it is recommended to use the built-in command policies discussed in the following section and to adhere to simple expressions as used in these examples to maintain policy readability.

2.6.4.7 Using the Built-in Command Policies

There are four default command policies available on the system to get started with. These four policies are enumerated in the table below along with each

policy's full command specification string as it would be entered on the command line.

Table 0-1.

Policy Name	cmdSpec Expression
read-only	(^show\s+(?!system)(?!ns ns.conf).*)|(^stat.*)
operator	(^show\s+(?!system)(?!ns ns.conf).*) | (^stat.*)|(^set.*-accessdown.*) | (^(enable|disable) (server|service).*)
network	^(?!shell)\S+\s+(?!system).*
superuser	.*

- The read-only policy allows all show commands, excluding the system command group and ns.conf show commands.
- The operator policy grants all of the read-only policy privileges and adds access to enable and disable commands on services. This policy also allows access to set services and servers as 'accessdown.'
- The network command policy permits near total system access excluding system commands and the shell command.
- Lastly, the superuser policy grants full system privileges, giving nsroot user identical privileges.

When using any of these built-in policies, you bind them as you would any other command policy. Binding of command policies is discussed in the next section.

2.6.4.8 Binding Command Policies

Once you have your command policies defined, you must bind them in order to put them in to use. When you create these bindings you must also set priorities on the policies to define their order of use. Command policies are evaluated in ascending order of assigned priorities.

Binding Command Policies per User

For this example, the user `johnd` created in section 2.6.3.1 and the previously listed example command policies will be reused. This example, in

combination with the group example that follows, creates a cumulative policy which will give system user johnd general but restricted access to the NetScaler CLI interface.

In this situation it is necessary to assemble command policies for a small set of users on a user by user basis. In system user johnd's case, he is to be granted feature level configuration access but not NetScaler system level access. To create this level of access, these three previously mentioned policies will be used.

```
> add system cmdPolicy deny_all_rm DENY "^rm.*"
> add system cmdPolicy deny_all_sh DENY "^shell"
> add system cmdPolicy deny_system_cmnd DENY "*.system.*"
```

When binding these policies system user johnd, priorities are assigned to define their order of evaluation.

```
> bind system user johnd deny_system_cmnd 1
> bind system user johnd deny_all_rm 5
> bind system user johnd deny_all_sh 10
```

The first command policy here will prevent johnd from accessing system level configuration commands. Next, he is disallowed access to the shell command in order to prevent modification at that level. Finally, the last policy will deny johnd all removal actions.

At this point, you may notice that by themselves, these policies are ineffective at restricting the user's access as the NetScaler system's default DENY command policy already restricts all user access to CLI commands. The group command policy example will resolve this and make user johnd's command policies valid.

Binding Command Policies per Group

Here again the group and user examples from section 2.6.3.1 are reused. Recall that the system user johnd was made a member of the nocusers system group. This example relies on johnd's group membership to create his overall user policy.

Using the `default_deny_override` policy created earlier and reused here, the system's DENY policy is overridden, allowing full NSCLI access.

```
> add system cmdPolicy default_deny_override ALLOW "^.*"
```

```
> bind system group nocusers -policyName
default_deny_override 100
```

Note again that the policy has been bound to the nocusers group with a priority of 100. This will ensure the ordering of the priority among any other policies that may later be bound against this group.

Now that all of the group and user command policies are in place, the complete order of policy evaluations for johnd can be explained. The user johnd's direct policies will be evaluated first, preventing access to system command group commands, remove actions and access to shell, in that order of priority. Due to his group membership, the user will otherwise have access to remaining commands because of the group's default deny override policy. The next section explains how the NetScaler's command policy evaluation procedure causes this overall policy order to achieve the desired level of user access for johnd.

2.6.4.9 Evaluation Process in Command Policy Application

As previously mentioned, a user's set of applicable command policies is an aggregate of their direct policies and those bound to them implicitly via group memberships. Every time a user enters a command, the system will search through the user's aggregate set of policies until it finds an explicit ALLOW or DENY action which matches the entered command. When a match is found, the system exits the command policy search after enforcing the defined action. If no matching policy is found, the user's access to the command is denied, per the system's default deny policy.

When applying policies to system users and groups keep in mind how the NetScaler system internally ties policies to users. Firstly, the system orders and executes policies based on assigned priorities, ordering user and group bindings together. In the case of user johnd above, if the policy bound to the nocuser group had been bound with a priority of 9 rather than 100, the system would have ordered that group policy before johnd's last policy which has a priority of 10. Secondly, when identical priorities are encountered between two command policies, the system orders them linearly. That is to say, these policies are evaluated in first in - first out order in regards to the when the policies were initially bound.

Note: Care must be taken when placing a user into multiple groups so that unintended user command restrictions or privileges are not inadvertently produced when the system aggregates policies for users.

In order to avoid these conflicts, keep in mind the command policy search procedure and policy ordering when using groups to organize your system users.

2.6.5 External Authentication for System Users

The NetScaler 9000 series supports the use of authentication policies for establishing external authentication of configured system users. Simple single server configurations can be created with policies by binding an authentication policy to the system global entity. In addition, a cascade of authentication servers can be configured by binding multiple policies to system global. If no authentication policies are bound to system users, system users are authenticated by the NetScaler onboard system.

Note: System users must be configured on the NetScaler system before external authentication can succeed for them. You must create an onboard system user for all those users who are to access the system in order to bind command policies to them. Regardless of authentication source, system users cannot log in if they are not granted minimally sufficient command authorization via bound command policies.

2.6.5.1 Creating an Authentication Policy

With the NetScaler authentication system, RADIUS, LDAP, TACACS+, and NT4 authentication systems are supported. For this example, a RADIUS based authentication server will be configured by the resulting policy. If another server type is needed in your configuration please refer to the appropriate 'add authentication' command in the NetScaler 9000 Series Command Reference" for complete relevant command details. The fundamental policy structure and creation procedure are the same regardless of authentication server type.

The first element needed to construct an authentication policy is an authentication action, which lists the server specific parameters. For a RADIUS server, the minimum parameters that the action must specify are the server's IP address and the RADIUS key. The example here shows how to create a RADIUS action.

```
> add authentication radiusaction NOC_RAD_Server
-serverip 10.125.0.25 -radkey nocknock
```

Other parameters may be necessary depending on the target RADIUS server's configuration. Please refer to the "NetScaler 9000 Series Command Reference" for complete details on other parameters for adding a RADIUS action.

Next, the policy itself can be created, tying it to the newly created action.

```
>  add authentication radiuspolicy NOC_RAD_POL  "ns_true"
NOC_RAD_Server
```

Note that you must also include an expression as part of the authentication policy. For authentication policies, only the 'ns_true' policy expression is supported.

2.6.5.2 Binding an Authentication Policy

Once the desired authentication policy is configured on the system, it must be bound to the system global entity with a priority in order to have the policy take effect.

```
> bind system global NOC_RAD_POL -priority 1
```

To create a cascade of authentication servers, all that is necessary is to create the desired policies and then bind each of them to the system global entity. To define the order of the cascade, bind the policies with increasing priority values so that the first policy to be evaluated has the lowest priority value.

Note that the onboard NetScaler authentication system is always consulted last in every user authentication process. Even in the case where only a single user authentication policy is bound to system global, the user will be authenticated against the onboard authentication mechanism if authentication with the policy-defined server fails.

2.6.6 Configuring DNS on the NetScaler System

If you need to enable DNS lookups on your NetScaler 9000 system you will need to do the following:

1. Execute the ‘shell’ command in the nscli.

2. Change to the /nsconfig directory with the ‘cd /nsconfig’ command.

3. Create a new file in this directory titled ‘resolv.conf’.

4. Open this file for editing using vi. Add a standard entry for a resolv.conf file as shown in the example below. Substitute the correct nameserver IP address and domain information for your network.

```
domain noc.company.com
nameserver      169.175.12.23
```

5. Save the file and exit the editor. Reboot the system to put the change into effect.

2.6.7 Configuring Clock Synchronization

To enable clock synchronization on your NetScaler system, follow the steps here to configure your system to utilize NTP (Network Time Protocol) for clock synchronization.

1. Copy the /etc/ntp.conf file to /nsconfig/ntp.conf.

2. Edit /nsconfig/ntp.conf and add the IP address for the desired NTP server under the 'server' and 'restrict' entries as indicated in the file.

3. Edit /nsconfig/rc.conf and add the text ntpd_enable="YES".

4. Reboot the system to apply your changes.

Note: If you do not have an NTP server to use for time synchronization, listings of public, or open access, NTP servers can be found at the official NTP site at http://www.ntp.org under the ‘Public Time Servers List’ pages. Be sure to read and adhere to the ‘Rules of Engagement’ page linked to on these pages before selecting a NTP server from the lists.

2.6.8 Using NetScaler 9000 Series Logging

The NetScaler system allows you to customize the logging of system events and SSL VPN access events, according to site needs. You can direct these logs either to local files on the NetScaler or to external log hosts. This section explains how to customize these logging aspects.

Note: After editing files to customize your NetScaler system's logging as discussed in this section, you must restart the system to activate the changes.

2.6.8.1 Logging NetScaler Events

To customize logging to fit site needs, configuration is modified for two functional areas - NetScaler messaging and syslog. The NetScaler system has an internal event message generator, which passes messages to the syslog system. The syslog system accepts these messages and performs the logging.

This section covers configuring NetScaler event messaging. The syslog configuration is discussed in the next section.

Note: For High Availability (HA) installations, the system logging configurations are not automatically propagated across an HA pair. You must manually copy the configurations over to an HA peer or otherwise duplicate the modifications on the peer.

Controlling NetScaler Event Messaging

By default, the passing of system and VPN events are enabled. To disable the passing of these messages, add the respective strings from below to the end of /nsconfig/rc.conf, each on a new line. If the file does not already exist, you will need to create it.

To disable system events messages, enter:

```
nssyslog_enable="NO"
```

To disable VPN events messages, enter:

```
nsvpnlog_enable="NO"
```

2.6.8.2 Configuring Syslog

This section explains how to modify the syslog configuration of your NetScaler system.

Toggling Syslog Functionality

The syslog daemon is enabled by default. Should you need to disable it, add this line to the /nsconfig/rc.conf file.

```
syslogd_enable="NO"
```

Changing the Logging Facilities

To customize the syslog configuration, begin by copying the base syslog.conf file from /etc to /nsconfig/syslog.conf. When the system reboots, the

dynamically generated /etc directory will be recreated and your customized syslog.conf file will be used in place of the base version.

a. System Logging Facility

NetScaler system messages are configured to use the syslog local0 facility, logging to /var/log/ns.log. To override this configured facility, you will need to make two edits. First, add the following line to /nsconfig/rc.conf. You will need to create a new file if one does not already exist. Replace the local facility value in the syslogfacility=0 parameter with the desired local facility level.

```
nssyslog_flags="-s syslogfacility=0 -s syslog=1 -d
eventwait"
```

For example, if you need to configure the local2 facility for system logs, your new entry for the syslogfacility value will read as 'syslogfacility=2'.

Next, you need to edit the syslog configuration to reflect the new value also. If you have not previously copied the /etc/syslog.conf file to the /nsconfig/ directory, do so now. Open the /nsconfig/syslog.conf file and change the following line to use the new local facility value.

```
local0.*                        /var/log/ns.log
```

For example, rather than 'local0.*', your new entry will be 'local2.*' if you are configuring the local2 facility for system logs.

Note: When editing the syslog.conf file, be sure to use tabs as field separators.

b. VPN Logging Facility

NetScaler VPN messages are configured to use the syslog local1 facility, logging to /var/log/nsvpn.log. To use another syslog local facility for VPN logging, you will need to change entries in two places as with the system logging facility.

First, edit the /nsconfig/rc.conf file, creating a new file if it does not already exist. In this file, add the following line, changing the syslogfacility value to your desired syslog local facility number.

```
nsvpnlog_flags="-s syslogfacility=1 -s syslog=1 -d
accesslogs"
```

If you are using local facility 4 rather than the default of 1, the syslogfacility entry needs to be changed to 'syslogfacility=4'.

Next, you need to update the /nsconfig/syslog.conf to reflect the new local logging facility value. To do this, edit the /nsconfig/syslog.conf file, changing the following line to use the new local facility value.

```
local1.*                        /var/log/nsvpn.log
```

For example, if you are configuring the local4 syslog facility for VPN event logging, the facility entry will need to be changed to 'local4.*' in this line.

Using a Log Host

If you prefer to have syslog send messages to an external log host rather than to local files, you need only to remove the log file specifications in your /nsconfig/syslog.conf file for either of the two local facilities, replacing them with the loghost hostname or IP address. The example below illustrates these changes.

```
local0.*                        @10.100.3.53
local1.*                        @10.100.3.53
```

You must also configure your loghost system to accept both local logging facilities for it to successfully receive both logs. Consult with your loghost system's documentation in order to confirm how to do this. For most UNIX based servers using standard syslog, you will need to add a local facility configuration line for both the ns.log and the nsvpn.log files in the syslog.conf configuration file. The facility values must correspond with those configured on the NetScaler system.

2.6.8.3 Log File Rotation

The log files present on the NetScaler system are rotated automatically at regular intervals. If you change the names of your log files, you will need to update the rotation configuration to reflect the names you are using so that the correct files will be rotated. Additionally, if you wish to customize the rotation configuration for the log files, you may do so. The file which controls log rotation can be found at /etc/newsyslog.conf.

To make changes to this file, copy the file from /etc/newsyslog.conf to /nsconfig/newsyslog.conf if one does not already exist at /nsconfig. Edit the newsyslog.conf file in /nsconfig and reboot when done in order to affect the changes.

If you need to update a log file name, edit the appropriate file name in the left most column. The remaining columns control the log rotation parameters. If you need to customize the log rotation parameters, please refer to the FreeBSD manpage on newsyslog(8) as this is the same format NetScaler system logging uses for its log rotation management.

2.7 Path MTU Discovery

Path MTU Discovery is a method for dynamically learning the maximum transmission unit (MTU) of any Internet path. This discovered Path MTU is then be used by the TCP or UDP layer to create packets of that size. This will avoid the fragmentation overhead on the routers in the path and reassembly overhead on the receiver.

PMTU Discovery is an operation mode in the NetScaler system. This mode enables the Netscaler system to inter-operate with other routers participating in PMTU Discovery. In a typical topology, the NetScaler system is deployed in front of the servers and either manages connection to the clients on behalf of the servers (transparent mode) or manages connections with the servers and clients independently (edge mode).

By default, the NetScaler system does not participate in Path MTU Discovery. This can be enabled by configuring the NetScaler system to operate in the PMTU Discovery mode. For more information on enabling the PMTUD mode using the NetScaler CLI, refer to the section Configuring PMTU Discovery in this chapter.

2.7.1 Behavior of the NetScaler System in Edge Mode

In edge mode, the NetScaler system manages connection to the server and the client separately. The following table lists the cases and the expected behavior of the NetScaler system on receipt of a PMTU related ICMP error message:

Table 4-1 Conditions and Behavior of the NetScaler System on Receipt of a PMTU related ICMP Error

No.	Condition	Behavior of the NetScaler System
1	For client connections, the NetScaler system uses an MSS of 1460 bytes. The MSS of the packets sent to the client is minimum of 1460 bytes as received from the client. While routing the packet if the network contains a router that fragments the packet into multiple datagrams because of MTU mismatches, an ICMP error is sent by the router.	The NetScaler system should parse the ICMP error and estimate a lower MTU appropriately for the path to that particular client. In this case, the ICMP error will not be passed to the server. The MTU database will be updated with the lower MTU. All new connections use the lowered MTU value from the database.

2.7.2 Behavior of the NetScaler System in Transparent Mode

In the Transparent mode, if the server sets the DF bit and sends a datagram, if the Path MTU is smaller than the size of the datagram, the ICMP error is received by the NetScaler system. The following table lists out the conditions and the expected behavior of the NetScaler system on receipt of a PMTU related ICMP error message:

Table 2-1 Conditions and Behavior of the NetScaler System on Receipt of a PMTU related ICMP Error

No.	Condition	Behavior of the NetScaler System
1	When the NetScaler system is in the MIP mode of operation.	Passing the ICMP error to the server will have the server adjust the MTU to the NetScaler MIP. This will affect all the clients using the same MIP to that particular server. Hence, the ICMP error is consumed by the NetScaler system and the MTU database is updated. All packets sent out on that connection would have the DF bit unset. All new connections will use the MTU value from the database.
2	When the NetScaler system is in the USIP mode of operation, and an ICMP error message is received.	The ICMP error message is translated and sent to the server. The server updates the MTU for the destination and subsequent datagrams go out with a lowered MTU. The MTU value for that client is also updated in the NetScaler system. All new connections use the lowered MTU value.

2.7.3 Configuring PMTU Discovery

- For enabling the Path MTU Discovery mode, use the following CLI command:

  `enable ns mode PMTUD`

- For disabling the Path MTU Discovery mode, use the following CLI command:

  `disable ns mode PMTUD`

2.8 Understanding NetScaler License Keys

The NetScaler 9000 Series supports the following licensed features:

- Load Balancing
- Content Switching
- Cache Redirection
- Centralized Web Logging
- SSL Acceleration
- Compression
- Surge Protection
- Sure Connect
- Priority Queuing
- Get flood (HTTP DoS) protection
- Content Filtering
- GSLB
- Proximity-based GSLB
- DNS
- SSL VPN (by feature and by concurrent users)
- Application Caching

Each of the products in the NetScaler 9000 Series includes a license key for some combination of these features (see Section The NetScaler 9000 Series on Page '5'for the details on the product you have purchased). This license key permits the user to ENABLE or DISABLE the purchased features on that system.

2.8.1 Implications of Enabling/Disabling Licensed Features

To enable or disable single or multiple features, the enable/disable feature commands are used.

For example:

- To enable the Load Balancing, Content Switching and Content Filtering features, type the following CLI command:

  ```
  enable feature lb cs cf
  ```

- To disable the Load Balancing feature, type the following CLI command:

  `disable feature lb`

Note:

1. If the license key is not available for a particular feature then the **`enable feature`** command does not enable the feature. The NetScaler 9000 system displays an error message: `ERROR: feature(s) not licensed`.
2. If multiple features are enabled at the same time, for example, **`enable feature lb cs cf`** and one of the feature does not have the license key, then the enable feature command will display an error for that feature.

2.8.2 Commands for the features that are enabled or disabled

Irrespective of whether a feature is enabled or disabled, you can use both the CLI and GUI to configure the licensed features. The feature configuration succeeds irrespective of whether the feature is enabled or disabled.

Note: When a feature is temporarily disabled and if you try to configure this feature using the CLI or GUI, the configuration succeeds.

The feature enabled or disabled check is done at runtime by NetScaler during it's normal operation and depending on whether a feature is enabled or disabled the appropriate feature specific run time behavior is enforced. The following section clarifies the run time behavior of each feature when the feature is disabled.

Note: The system displays warning message when the user tries to configure a disabled feature. The feature names are acronyms, as used in the **`enable feature`** command.

The warning message is used to notify the user that, although the requested configuration action has been made, the corresponding feature is not currently enabled; the command will have no effect on the runtime behavior of the NetScaler 9000 system until the feature is enabled.

An error message is displayed when the user tries to configure an unlicensed feature.

The error message indicates that the requested configuration action is not possible because the license for the corresponding feature is not installed on the NetScaler 9000 system.

2.8.2.1 NetScaler Runtime enforcement of a feature that is disabled

- Load Balancing (LB)

  The load balancing policy is not enforced when the LB feature is disabled. All client requests are sent to the first service that is bound to the load balancing vserver. If this first service is reported down by the monitor bound to it, then the vserver is also marked as down.

- SSL Acceleration: No SSL Acceleration is provided when the SSL feature is disabled.
- Compression (CMP): No compression is done by the NetScaler when the CMP feature is disabled.
- Content Switching (CS) - A HTTP 503 “HTTP/1.1 Service Unavailable” response is returned to the client.
- Cache Redirection (CR)
  - For Transparent mode, all requests are sent to the origin Server.
  - For a Reverse or a forward proxy mode, a HTTP 503 “HTTP/1.1 Service Unavailable” response is returned to the client.
- Content Filtering (CF)

  No Content Filtering will be done, that is, there will be zero hits on the configured filters.

- SureConnect (SC)- Sure connect feature is not triggered.
- Priority Queuing (PQ)

  There will be no Priority queues based on the policies configured. All requests will be either request switched to the service or will be queued onto the Surge Queue.

- HTTP DOS (HDOSP) - The HTTP DOS protection feature is not triggered.
- Global Server Load Balancing (GSLB) -

- When GSLB feature is *enabled*, the DNS response generated by NetScaler runs through the GSLB decision-making mechanism. This mechanism re-orders the IP addresses in the list based on the health metrics of each IP address.
- When GSLB feature is *disabled*, the IP addresses are not re-ordered. The system will maintain a list of IP addresses in the order in which they were configured on the NetScaler 9000 system.

- Proximity-based GSLB - The Proximity base GSLB feature cannot be enabled separately. The license hierarchy is:
  - Proximity needs base GSLB and base GSLB in turn requires LB. For GSLB, the DNS support to add domains is required.

    So for the Proximity based GSLB to work, you need to have Base GSLB, Proximity based GSLB, LB and DNS licenses.
- Web Logging (WL): No Web logging will be done, that is, the log files are not created.
- Surge Protection (SP)- The Surge Protection feature is not triggered.
- SSL VPN – The SSL VPN feature is enabled by default for 5 licensed users. If the number of concurrent user sessions exceeds this limit then NetScaler returns the error message “SSLVPN - Number of users exceeded.” Additional user packs are available as a means of boosting the number of concurrent user sessions supported.
- Integrated Cache or Application Caching – To trigger Static and Dynamic caching, the user has to enable the Integrated Cache feature. When the Integrated Cache feature is enabled, basic Static caching is performed. To cache dynamic contents, the user has to configure Dynamic caching in the NetScaler 9000 system.

2.9 Autodetect Service

When the NetScaler 9000 system is deployed in transparent mode, it provides autodetect service where it automatically detects the backend web servers. Some of the scenarios are:

2.9.1 Global HTTP port configuration

In this case, in the transparent mode connection multiplexing you can configure global HTTP port(s) on the NetScaler 9000 system with no virtual IP addresses (VIPs) or services.

The global HTTP port(s) can be configured using the following command at the CLI prompt:

set ns config -httpPort 80

In this case, the client directly accesses the backend web servers using the server's IP address. If the destination port matches with the configured global HTTP port(s) then the NetScaler 9000 system dynamically detects and learns the information about the servers running at the backend.

2.9.2 Cache-Redirection Configuration

In this case, the NetScaler 9000 system is deployed in transparent or reverse Cache Redirection topology and the Cache Redirection Virtual server mode is set to Cache. On detecting the Cache down, the requests are automatically redirected to the origin server(s).

2.9.3 Transparent SSL Configuration (*:443)

In this case, in the transparent mode connection multiplexing configure wildcard *.443 port(s) on the NetScaler 9000 system with no virtual IP addresses (VIPs) or services.Use the following command at the CLI prompt:

add vserver <vServerName> SSL * 443

In this case the client directly accesses the backend web servers using the server's IP address. If the destination port matches with the configured wildcard *.443 port(s) then the NetScaler 9000 system dynamically detects and learns the information about the servers running at the backend.

Chapter 3
High Availability

This chapter introduces you to the NetScaler 9000 system High availability configuration setup. It also provides the steps to configure the NetScaler 9000 system in high availability mode.

Topics included are

- Overview
- Considerations for High Availability Setup
- Configuring two NetScaler 9000 systems in High Availability Mode
- Changing to a High Availability Configuration
- Verifying Configuration Propagation
- Force Failover of the Primary NetScaler 9000 System
- Forcing the Secondary Device to Stay Secondary
- Troubleshooting HA Issues

3.1 Overview

If the NetScaler 9000 system deployed in a stand alone mode stops functioning due to unexpected network error then your network will be unavailable to traffic till the network error is resolved. To avoid this problem you can deploy two NetScaler 9000 systems in the network; on failure of one system the other NetScaler 9000 system acts as a backup and keeps the network alive for the traffic. This mode of having one NetScaler 9000 system as a backup for the other is called the High Availability mode.

In this mode, one NetScaler 9000 system is configured as the Primary (active) and the other is configured as Secondary (passive). The secondary NetScaler 9000 system sends periodic '*hello*' messages to the primary NetScaler 9000 system to check whether it is operating. If the secondary does not receive a reply, it sends successive "hello" messages. If there is no response for a

specified time period, it determines that the primary NetScaler 9000 system is not functioning normally and fail over occurs.

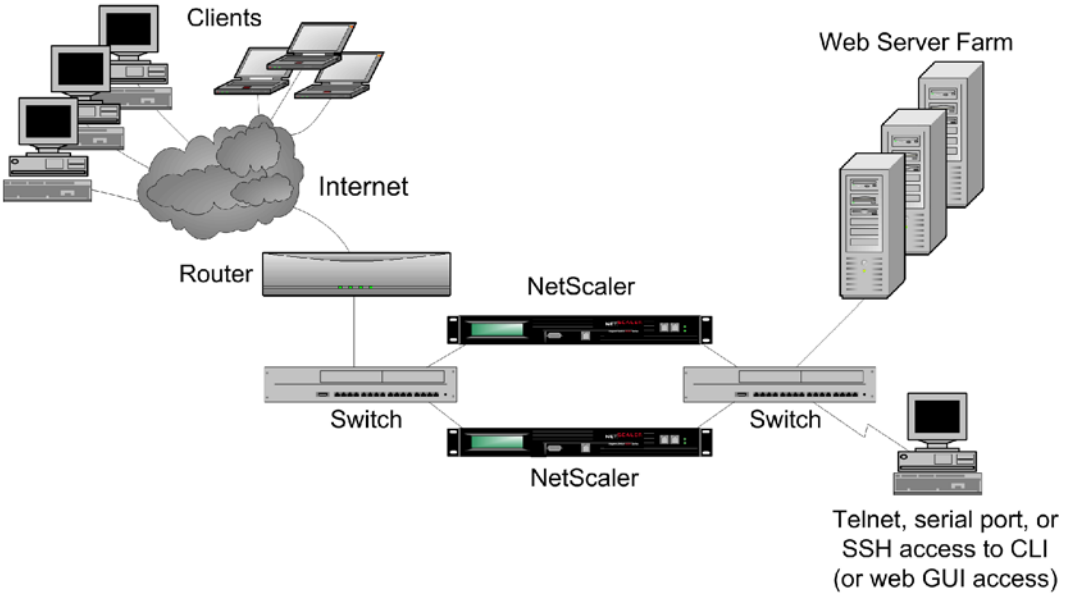
After the fail over, all client connections must be re-established but the session persistence rules are maintained as they were before fail over.

Note: If the web server logging feature is enabled after fail over this feature remains enabled on the NetScaler that has taken over as primary. That is, no log data is lost due to failure of the primary NetScaler. For this scenario the log server configuration must carry entries for both the NetScaler systems in the `log.conf` file.

Figure 3-1 shows a network configuration that uses the high availability feature. Hubs may be used instead of switches.

Note: If hubs are used, check the interface and duplex settings on the NetScaler 9000system

Figure 3-1 NetScaler 9000 system in High Availability mode



3.2 Considerations for High Availability Setup

To configure NetScaler 9000 systems for High Availability (HA) mode, consider the following points.

1. In HA mode, when the password of the **nsroot** user account is changed on either system, the change must also be performed on the peer as password synchronization is required.
2. The configuration file (`ns.conf`) on the primary NetScaler 9000 system and the configuration file (`ns.conf`) on the secondary NetScaler 9000 system must match with following exceptions:
   - The Primary and Secondary NetScaler 9000 system must be configured with unique System IP addresses (NSIP).

     Use the **ns config** CLI command to configure or modify the NSIP address.
   - The Node ID and associated IP address must reflect peer's Node ID and IP addresses.

     For example, if there are two NetScaler 9000 systems *NS1* and *NS2* then NS1 must be configured with a unique node ID and IP address of *NS2* and NS2 must be configured with a unique node ID and IP address of *NS1*.
3. Common configuration files may need to manually synchronized. On both units in an HA setup, there may be a need to have a set of common configuration files depending on the deployment needs.

   For example, if SSL offload is enabled, then SSL certificates must be placed at the same location (directory) on both the NetScaler units. Similar examples include `vsr.html` (for Sure Connect), any manually-customized files, or any other batch files containing configuration commands.
4. The RPC node passwords must be configured on HA systems. Initially, all NetScaler systems are configured with the same RPC node password. It is highly recommended that users change the RPC node passwords on their NetScaler systems. RPC nodes are implicitly created by the **add ns node** and **add gslb site** commands. There is no need or means to create or delete RPC nodes explicitly.

   To change an RPC node password use the **set rpcnode <IP_address> -password <PASSWORD>** command. The **IP_address argument** is the IP address of the peer NetScaler with which this NetScaler is to communicate. The **PASSWORD** argument is the

password with which this NetScaler will be authenticating, given by IP_address.

To view the list of RPC nodes use the command **`show rpcnodes`**. Passwords shown by this command are encrypted and will be stored in the the ns.conf file this way.

RPC nodes are internal NetScaler entities that are used for NetScaler to NetScaler communications, as in HAcommunications of configuration and session information. To communicate with other NetScaler systems, each NetScaler requires knowledge of those systems it it is to communicate with and how to authenticate on the peer NetScaler. RPC nodes maintain this information, which includes the IP address of the peer NetScaler and the password used for authentication on the peer. One RPC node exists on each NetScaler peer. This node stores the password, which is checked against the one provided by the contacting NetScaler.

3.2.1 One-Arm Mode Configuration Considerations

If the NetScaler 9000 systems in a high availability setup are used in one-arm mode, disable all NetScaler 9000 system interfaces except for one that is connected to the switch or hub.

Use the **`disable interface`** CLI command to disable interfaces.

3.2.2 Mapped IP Address Configuration Considerations

When you configure the NetScaler 9000 system, make sure that the mapped IP address of both the primary and the secondary NetScaler 9000 system is exactly the same.

If needed, you can change the mapped IP address at any time by running the NetScaler 9000 system's configuration program.

Note: For more information on changing the mapped IP address, refer to Chapter 2: Installation, Configuration and Management.

The following procedures show an alternate method of adding/changing the mapped IP addresses. You can use these procedures if you have Telnet/SSH access to one or both NetScaler 9000 systems.

3.2.2.1 Adding or changing the Mapped IP address using Telnet or SSH

- **Telnet/SSH access to both the NetScaler 9000 systems**

  Use this procedure if you have Telnet access and/or SSH access only to both the NetScaler 9000 systems:

  1. Enter the **`ns config`** CLI command on the first NetScaler 9000 systems.
  2. The configuration menu is displayed. In the menu use the menu item 4 to change the mapped IP address.

  Note: Do not add server, services and other configurations while changing the NetScaler 9000 system's basic configuration using the **`ns config`** command.

  3. In the configuration menu, use menu item 6 to save changes and exit.
  4. Repeat steps 1 to 3 for the second NetScaler 9000 system.
  5. Reboot both NetScaler 9000 systems.

- **Telnet/SSH Access to One of the NetScaler 9000 system**

  Use this procedure if you have Telnet access and/or SSH access only to one of the two NetScaler 9000 systems:

  1. Telnet to the NetScaler 9000 system's IP address of one of the NetScaler 9000 systems.
  2. Enter the **`ns config`** CLI command on this NetScaler 9000 system.
  3. The configuration menu is displayed. In the menu, use the menu item 4 to change the mapped IP address.

  Note: (Do not add server, services and other configurations while changing the NetScaler 9000 system's basic configuration using the **`config ns`** command.)

  4. In the configuration menu, use menu item 6 to save changes and exit.
  5. On the reboot message - ***do not reboot.***

6. Telnet from this NetScaler 9000 system to the other NetScaler 9000 system.
7. Repeat steps 2 to 4 for the second NetScaler 9000 system.
8. Reboot the second NetScaler 9000 system.

Note: This disconnects the Telnet session to the other NetScaler 9000 system and you will be returned (still logged in) to the first NetScaler 9000 system.

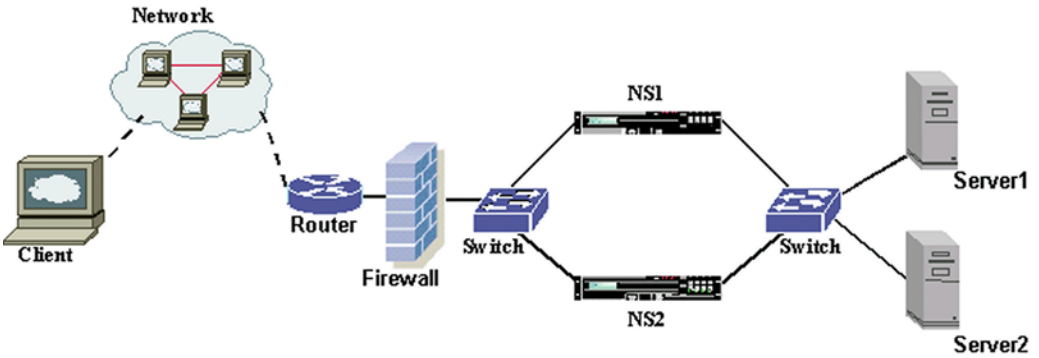
9. Reboot the first NetScaler 9000 system.

3.3 Configuring two NetScaler 9000 systems in High Availability Mode

This section describes the configuration steps to connect two NetScaler 9000 systems in High availability Mode as shown in Figure 3-2

With these configuration steps you can configure the one NetScaler 9000 system as Primary and the other NetScaler 9000 system as Secondary.

Figure 3-2 NetScaler 9000 system Connected in the High Availability Mode



3.3.1 Pre-configuration Steps

1. Perform the steps mentioned in the section Considerations for High Availability Setup.
2. Disconnect the NetScaler 9000 systems from the switches.

3.3.2 Configuration Steps

3.3.2.1 Configuring First NetScaler 9000 system (NS1)

1. Log-in to the NetScaler 9000 system using valid *Username* and *Password* on the *first* NetScaler 9000 system.

Note: If the NetScaler 9000 system is not pre-configured then you must define the system configuration by entering the **`/netscaler/nsconfig`** command at the shell prompt.

2. If you want to modify the present system IP address type **`ns config`** on the Command Line Interface (CLI)

   —Or—

   If you want to continue with the pre configured system IP address then jump to Step 4.

3. At the **reboot** prompt, type **`yes`**.

4. Enter the following command in the CLI.

   `add node <id> <ipAddress>`

   where in the

   - **`id`**: specify the unique node number for the *second* NetScaler 9000 system (NS2).
   - **`ipAddress`**: specify the IP address of the *second* NetScaler 9000 system (NS2).

   For the example shown in Figure 3-2 on page 6, add the Node ID as `1` and the IP address as `10.102.1.2`.

Note: The maximum node ID for NetScaler 9000 systems in a high availability setup is 64.

5. To disable those interfaces in the NetScaler 9000 system that are not connected or not being used for traffic, enter the following CLI command:

   `disable interface <ifnum>`

   where

- **<ifnum>**, is the number of the interface to be disabled in the NetScaler 9000 system (NS1).

Note: Repeat step 5 for each NetScaler 9000 system interface that will not be used.

6. To disable monitoring for those interfaces whose failure should not cause a *failover* in the HA mode, enter the following command in the CLI.

   set interface <ifnum> -hamonitor OFF

   where

   - **ifnum** is the number of a NetScaler 9000 system interface in the NetScaler 9000 system (NS1).

Note: Repeat step 6 for each NetScaler 9000 system interface that will be used and whose failure should not cause fail over.

7. To save the configuration enter **save config** in the CLI.
8. Connect the *first* NetScaler 9000 system (NS1)to the switches.

3.3.2.2 Configuring Second NetScaler 9000 system (NS2)

1. Log-in to the NetScaler 9000 system using your *Username* and *Password* on the second NetScaler 9000 system.

Note: If the NetScaler 9000 system is not pre-configured then you must define the system configuration by entering the **/netscaler/nsconfig** command at the shell prompt.

2. If you want to modify the present system IP address type **ns config** on the Command Line Interface (CLI)

   —Or—

   If you want to continue with the pre configured system IP address then jump to Step 4.

3. At the **reboot** prompt, type **yes**.
4. Enter the following command in the CLI.

   add node <id> <ipAddress>

where in the

- **id**: specify the unique node number for the *first* NetScaler 9000 system (NS1).
- **ipAddress**: specify the IP address of the *first* NetScaler 9000 system (NS1).

For the example shown in Figure 3-2 on page 6, specify the Node ID as `2` and the IP address as `10.102.1.1`.

Note: The maximum node ID for NetScaler 9000 systems in a high availability setup is 64.

5. To disable those interfaces in the NetScaler 9000 system that are not connected or not being used for traffic, enter the following CLI command:

   disable interface <ifnum>

   where

   - **<ifnum>**, is the number of the interface to be disabled in the NetScaler 9000 system (NS2).

Note: Repeat step 5 for each NetScaler 9000 system interface that will not be used.

6. To disable monitoring for those interfaces whose failure should not cause a *failover* in the HA mode, enter the following command in the CLI.

   set interface <ifnum> -hamonitor OFF

   where

   - **ifnum** is the number of the interface to be disabled in the NetScaler 9000 system (NS2).

Note: Repeat step 6 for each NetScaler 9000 system interface that will be used and whose failure should not cause fail over.

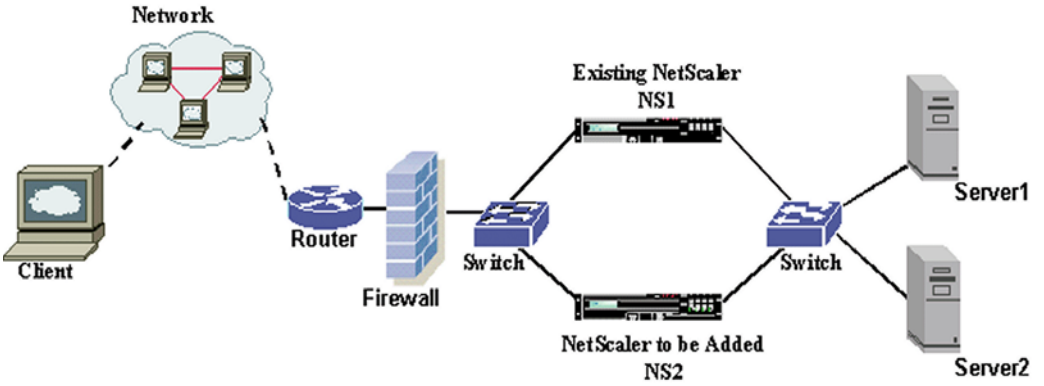
7. To save the configuration enter **save config** in the CLI.
8. Connect the *second* NetScaler 9000 system (NS2) to the switches.

3.4 Changing to a High Availability Configuration

This section describes the configuration steps to connect a new NetScaler 9000 system to a standalone NetScaler 9000 system in High Availability mode as shown in Figure 3-3.

With these configuration steps you can add the NetScaler 9000 system (*NS2*) to the stand alone NetScaler 9000 system (*NS1*) and also configure *NS1* to be in Primary mode and *NS2* to be in Secondary mode.

Figure 3-3 Adding a NetScaler 9000 system to a Standalone Configuration



3.4.1 Configuration Steps

3.4.1.1 Configuring the Existing NetScaler 9000 system (NS1)

1. Log in using **`nsroot`** as the *User Name* and *Password* on the NetScaler 9000 system *NS1*.
2. Enter the following command in the CLI

   `add node <id> <ipAddress>`

   where in the

   - **`id`**: specify the unique node number for the *second* NetScaler 9000 system (NS2) that needs to be added.
   - **`ipAddress`**: specify the IP address of the *second* NetScaler 9000 system (NS2), the NetScaler 9000 system that needs to be added.

   For the example shown in Figure 3-3 add the Node ID as `1` and the IP address as `10.102.1.2`.

Note: The maximum node ID for NetScaler 9000 systems in a high availability setup is 64.

3. To save the configuration enter **`save config`** in the CLI.
4. Verify the configuration using the following CLI command:

   `show node`

   This displays the Node ID, IP Address and Configuration mode for both NS1 and NS2. The following should be the display:

```
> show node
        2 configured nodes:
1)      Node ID:      0
        IP:    10.102.3.210
        Node State: UP
        Master State:  Primary
        Sync  State: Enabled
        Enabled Interfaces : 1/2 1/1
        Disabled Interfaces : None
        HA MON ON Interfaces : 1/2 1/1
        SSL Card Status: UP
2)      Node ID:      1
        IP:    10.102.3.201
        Node State: UNKNOWN/DOWN
        Master State:  Unknown
        Sync  State: Unknown
        Enabled Interfaces: Unknown
        Disabled Interfaces : Unknown
        HA MON ON Interfaces : Unknown
        SSL Card Status: Unknown
 Done
```

3.4.1.2 Configuring the Second NetScaler 9000 System (NS2)

1. Disconnect the NetScaler system from the network.
2. Log in using **`nsroot`** as the user name and password on the *second* NetScaler 9000 system *NS2*.

Note: If the NetScaler 9000 system is not pre-configured then you must define the system configuration by entering the **`/netscaler/nsconfig`** command at the shell prompt.

3. If you want to modify the present system IP address type **`ns config`** on the Command Line Interface (CLI)

   —Or—

   If you want to continue with the pre configured system IP address then jump to Step 4.
4. At the **reboot** prompt, type **`yes`**.
5. When the Secondary device is UP, set the Secondary node independent of the Primary node, using the following command:

   set node -hastatus STAYSECONDARY
6. Enter the following command in the CLI.

   `add node <id> <ipAddress>`

   where in the

   - **`id`**: specify the node number of the *first* NetScaler 9000 system (NS1).
   - **`ipAddress`**: specify the IP address of the *first* NetScaler 9000 system (NS1).

   For the example shown in Figure 3-3 on page 10 specify the Node ID as `2` and the IP address as `10.102.1.1`.

Note: The maximum node ID for NetScaler 9000 systems in a high availability setup is 64.

7. To disable those interfaces in the NetScaler 9000 system that are not connected or not being used for traffic, enter the following CLI command:

   `disable interface <ifnum>`

where

- **<ifnum>**, is the number of the interface to be disabled in the *second* NetScaler 9000 system (NS2).

Note: Repeat step 5 for each NetScaler 9000 system interface that will not be used.

8. To disable monitoring for those interfaces whose failure should not cause a *failover* in the HA mode, enter the following command in the CLI.

   set interface <ifnum> -hamonitor OFF

   where

   - **ifnum** is the number of a NetScaler 9000 system interface in the *second* NetScaler 9000 system (NS2).

Note: Repeat step 6 for each NetScaler 9000 system interface that will be used and whose failure should not cause fail over.

9. To save the configuration enter **save config** in the CLI.
10. Connect the *second* NetScaler 9000 system (NS2) to the network
11. Verify the configuration using the `show node` command:

Note: Verify the status of the synchronization process by typing the show node command after a few seconds. If the "Success: Synchronization succeeded" message is displayed, perform the next step.

12. To make the HA status of NS2 node active, use the following CLI command:

    set node -hastatus ENABLE

13. Execute the `save config` command.

3.5 Verifying Configuration Propagation

In a correct setup any command issued on primary NetScaler 9000 system *NS1* must propagate automatically to secondary NetScaler 9000 system *NS2*.

For example, on primary NetScaler 9000 system *NS1* type the following CLI command

```
add lb vserver Server1 http 10.102.1.1 80
```

- To verify if the new server **Server1** is added in NS1, type the following command at the CLI prompt on NS1:

  ```
  show lb vserver
  ```

  This lists all the Load Balancing virtual servers present in NetScaler 9000 system *NS1*. Check that the new server **Server1** is displayed in this list.

- To verify the configuration propagation, on the secondary NetScaler 9000 system *NS2*, type the following command at the CLI prompt on NS2:

  ```
  show lb vserver
  ```

  Check that the new server **Server1** that was added in NetScaler 9000 system *NS1* is displayed in the existing Load Balancing virtual server list in *NS2*.

3.5.1 Command Propagation Failure

The following are some of the command propagation failures and their work arounds:

If a command propagation fails, the network connectivity between primary and secondary NetScaler devices should be checked.

If a command execution succeeds on the primary NetScaler device but fails to propagate on the secondary NetScaler device, run the command again on secondary NetScaler device to see the exact error message. The error may have occurred because the resources required by the command are present on primary NetScaler device and are not available on the secondary NetScaler device.

If the authentication failure error is displayed, verify if the user `nsroot` exists on both primary and secondary NetScaler devices and if the password for the user is the same on both the primary and the secondary NetScaler devices.

3.6 Forced Synchronization

In addition to the automatic synchronization, the NetScaler system allows for a forced synchronization between two nodes in an HA setup. To force

synchronization between the nodes in an HA pair, you need to execute the Force Sync command.

You can execute this command both on the primary and secondary nodes. However, if synchronization is already in progress, the command will not work and the NetScaler system will display a warning.

This command will not work when:

- Executed on a standalone NetScaler system
- HA is disabled on the NetScaler system
- HA synchronization is disabled on the NetScaler system

The "Done" message displayed after you execute the force sync command does not indicate that the synchronization has been successful. To verify whether the operation has been successful, execute the `show node` command. This command indicates whether the nodes are synchronized.

3.7 Force Failover of the Primary NetScaler 9000 System

Force fail over is used to forcibly make the Secondary device take over as the Primary device. For example, lets have an existing HA setup where Machine A is the Primary device and Machine B is Secondary device. If there is a requirement to upgrade Machine A with a hardware component, then Machine B should take over and function as the primary device until Machine A is upgraded. To accomplish this the **`force ns fail over`** CLI command is used. This command can be executed from the Primary or the Secondary device.

Note: If the **`force ns failover`** CLI command is executed on a Standalone, it returns the error message "Operation not permitted on Standalone node."

The **`force ns failover`** CLI command will not be propagated or synchronized. There is no dependency between the **`force ns failover`** CLI command and synchronization. Synchronization will happen automatically whenever there is a change in the Primary. To see the status of synchronization after Force Failover, execute the **`show ns node`** CLI command to see if there are any errors in the synchronization process.

Note: When the **`force ns failover`** CLI command is executed on the Primary device, and the secondary device has been configured to stay as secondary using the **`set ns node –hastatus staysecondary`** CLI, then the system displays the error message "Operation not possible due to invalid peer state. Rectify and retry."

3.7.1 Executing Force Failover from the Primary Device

When the **`force ns failover`** CLI command is executed from Primary device, then this device becomes the Secondary device and the Secondary device becomes the Primary device. Force failover happens only if the Primary device gets the information that the Secondary device is UP.

Note: If the Secondary device is down, the **`force ns failover`** CLI command returns the error message "Operation not possible due to invalid peer state. Rectify and retry."

If the Secondary device is in claiming or inactive state, it returns the message "Operation not possible now. Please wait for system to stabilize before retrying."

3.7.2 Executing Force Failover from the Secondary Device

When the **`force ns failover`** CLI command is executed from Secondary device, then the Secondary device becomes the Primary device and the Primary device becomes the Secondary device. Force failover happens only if the Secondary device's health is good or if the device is not configured to stay secondary.

Note: If the Secondary device cannot become the Primary device or if Secondary device is configured to stay secondary using the **`set ns node -hastatus staysecondary`** CLI command, the system displays the message "Operation not possible as my state is invalid. Use show node for more information."

3.7.3 Enabling and Disabling Synchronization

To ensure that the Secondary node does not synchronize its configuration with that on Primary node whenever there is a change in the Primary, use the following CLI command:

set ns node –hasync DISABLE

To enable synchronization again, use the following command:

set ns node –hasync ENABLE

3.8 Forcing the Secondary Device to Stay Secondary

In an HA setup, the Secondary node can be forced to stay as a secondary device independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgrade, it is possible that the Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node.

The following is the CLI command to set the Secondary mode independent of the other unit in the HA setup:

set ns node –hastatus STAYSECONDARY

The unit on which this command is issued will remain as Secondary even if the Primary fails for some reason. If the **`-hastatus`** of a unit is made stay secondary, this device does not participate in HA State Machine transactions. The **`show node`** CLI command will display the status of this node as "HA SUSPENDED".

The **`set ns node –hastatus STAYSECONDARY`** CLI command works on a standalone node and a Secondary node. In a standalone node, this command has to be executed before running the **`add node`** CLI command. When a new node is added, the existing node will stop processing traffic and functions as the Secondary node.

Note: If the **`set ns node –hastatus STAYSECONDARY`** CLI command is executed on a secondary node, it will not become the Primary node even if there is a failure in the Primary node.

The **set ns node** command will not be propagated or synchronized, and affects only the node on which the command is executed.

To ensure that the unit is put back as an active HA unit, use the following command:

set ns node –hastatus ENABLE

3.9 Troubleshooting HA Issues

This section provides troubleshooting information for some of the existing High Availability feature issues.

1. Improper synchronization of VLAN Configuration in High Availability NetScaler 9000 systems

   Ensure that the VLAN configuration is done after configuring the NetScaler 9000 system with the High Availability setup.

   For NetScaler 9000 systems in High Availability setup, synchronization does not work properly when only one NetScaler 9000 system has a VLAN configuration.

2. Retrieving lost configuration

   If the primary NetScaler 9000 system is unable to send the configuration to the secondary NetScaler 9000 system because of any network error then the secondary NetScaler 9000 system may not have an accurate configuration and may not behave correctly if failover occurs.

   In this situation, you can retrieve the original primary NetScaler 9000 system's configuration from a back-up copy present in the NetScaler 9000 systems disk. The NetScaler 9000 system saves the last four copies of the `ns.conf` file in the `/nsconfig` directory. These are named `ns.conf.0`, `ns.conf.1`, and so on. The `ns.conf.0` file contains the latest configuration.

   To retrieve the NetScaler 9000 system's configuration, proceed as follows:

   a. Exit from the CLI to FreeBSD by entering this CLI command:

      ```
      >shell
      ```

   b. Enter the following FreeBSD commands to determine the name of the latest backup copy (based on the timestamp of the file):

      ```
      #ls -lt /nsconfig/ns.conf.? | head -1
      ```

OR

```
#ls -ltr /nsconfig/ns.conf.? | tail -1
```

c. Copy the latest backup file to `/nsconfig/ns.conf`.

```
#cp /nsconfig/ns.conf.0 /nsconfig/ns.conf
```

3. Configuration done via `NSConfig` utility is not propagated. Any configuration done using `NSconfig` has to be done on each node.

Chapter 4
NetScaler Statistical Utility

This chapter introduces you to the NetScaler Statistical Utility (also referred to as NetScaler Dashboard). It explains the various components of this graphical utility and illustrates steps to monitor NetScaler 9000 system's performance using the Dashboard utility.

Topics included are:

- Overview
- Accessing NetScaler Dashboard
- Understanding Graphs and Legends
- Dashboard Components
- Monitoring Performance Statistics of Key NetScaler Features

4.1 Overview

NetScaler Statistical Utility (referred to as Dashboard) is a highly intuitive graphical utility that allows users to monitor real-time performance of the NetScaler 9000 system with the use of graphs and tables. The statistical data that is retrieved by NetScaler Dashboard provides the structure to analyze and interpret the performance of the NetScaler 9000 system. The NetScaler Dashboard visually formats the statistical data on a real-time basis, to facilitate quick comprehension of the state of the NetScaler 9000 system. Using the visual formats provided, the user can view the NetScaler performance data in graphical, or tabular form.

The users can monitor the quality of service for NetScaler's key features like Load Balancing, Content Switching, Interfaces and SSL VPN. Apart from other custom-design graph components and tables, NetScaler Dashboard has the ability to display 3 graphs in one frame. Each graph can monitor various feature-specific performance statistics, including the packet rates, hits rate, Client and Server connection rates and current SSL VPN sessions. The utility provides an option to the users to chose and plot any global statistic

(monitored by NetScaler system) belonging to various protocols, versus others.

Note: Some of these features are dependent on the licenses that are enabled on the NetScaler system.

4.2 Accessing NetScaler Dashboard

NetScaler Dashboard is a web-based applet. This applet minimally requires version 1.3.1_01 of the Java® applet plug-in.

4.2.1 System Requirements

The system requirements for the computer on which the NetScaler Dashboard will be running are as follows:

Windows

Pentium® 166 MHz or faster processor with at least 48 MB of RAM is recommended for applets running in a browser using a Java plug-in product. You should have 40 MB free disk space before installing the plug-in.

Linux

A Pentium platform running Linux kernel v2.2.12 and glibc version 2.12-11 or later. A minimum of 32 MB RAM is required. Recommended 48 MB RAM, 16-bit color mode, KDE and KWM window managers used in conjunction with displays set to local hosts.

Solaris

The Java 2 Runtime Environment, Standard Edition, version 1.3.1_01 is intended for use on Solaris 2.6, Solaris 7 and Solaris 8 operating environments.

Prior to installing the Java 2 Runtime Environment, insure that you have installed the full set of required patches needed for support of this release.

See the “Solaris Patch Installation” section before proceeding. See also “Solaris Font Package Requirements” section for information about font packages which should be on your system.

4.2.2 Invoking NetScaler Dashboard

To invoke NetScaler Dashboard from your web browser:

1. Type the URL in the following format:

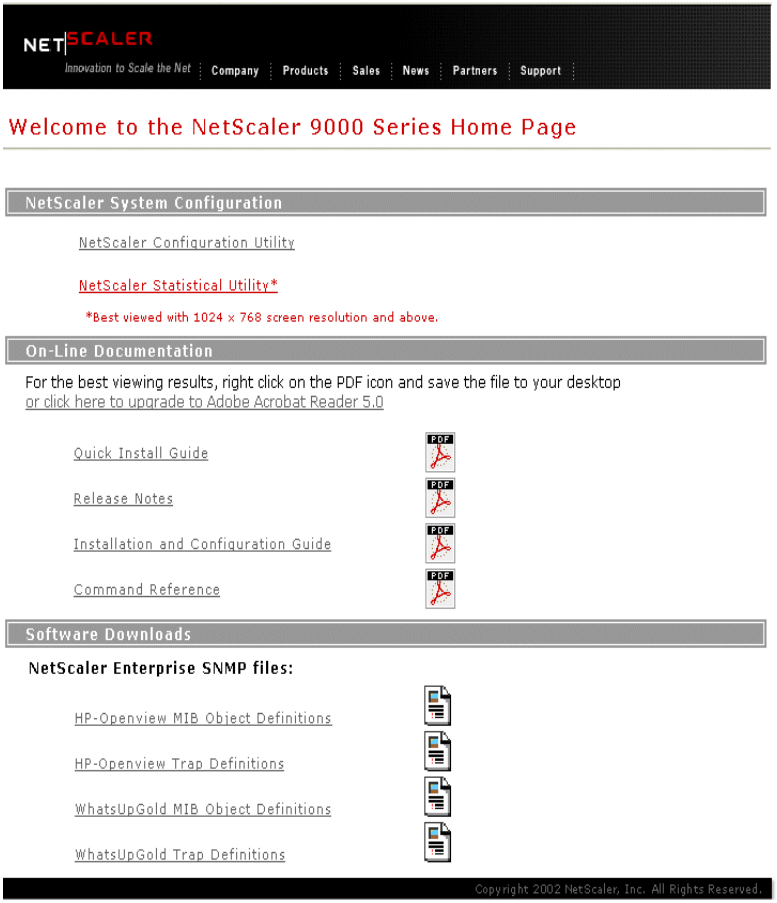
   http://*IP_address_of_NetScaler 9000 system*

   For example, if IP address of the NetScaler 9000 system is 192.168.10.1, enter the following in the browser's address field:

   `http://192.168.10.1`

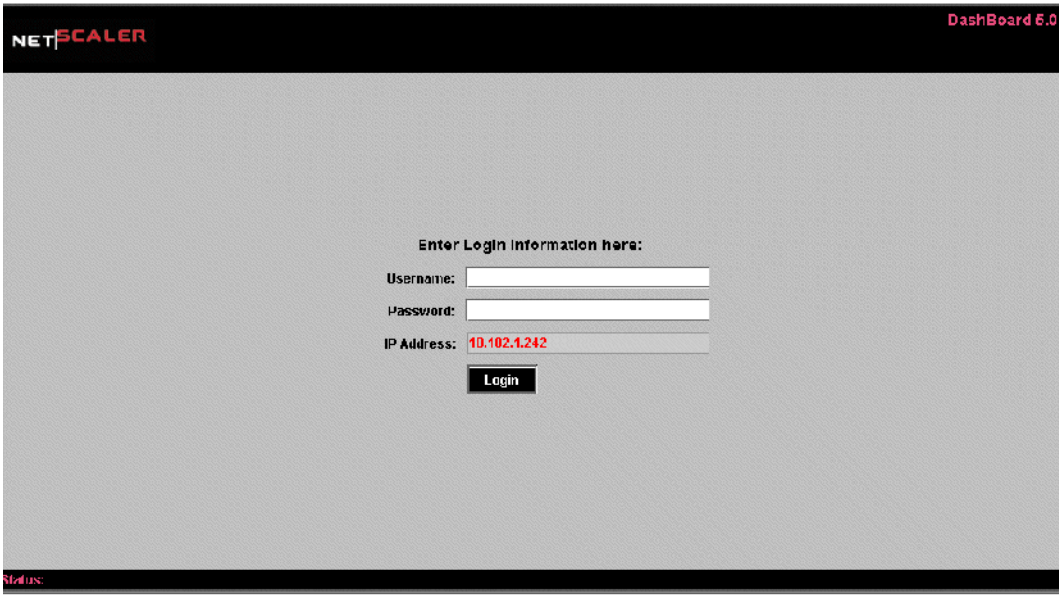
2. Press the <`Enter`> key, the following NetScaler 9000 Series Home Page is displayed.

Figure 4-1 NetScaler 9000 Series Home Page.


NETSCALER
Innovation to Scale the Net
Company
Products
Sales
News
Partners
Support
Welcome to the NetScaler 9000 Series Home Page
NetScaler System Configuration
NetScaler Configuration Utility
NetScaler Statistical Utility*
*Best viewed with 1024 x 768 screen resolution and above.
On-Line Documentation
For the best viewing results, right click on the PDF icon and save the file to your desktop
or click here to upgrade to Adobe Acrobat Reader 5.0
Quick Install Guide
Release Notes
Installation and Configuration Guide
Command Reference
Software Downloads
NetScaler Enterprise SNMP files:
HP-Openview MIB Object Definitions
HP-Openview Trap Definitions
WhatsUpGold MIB Object Definitions
WhatsUpGold Trap Definitions
Copyright 2002 NetScaler, Inc. All Rights Reserved.

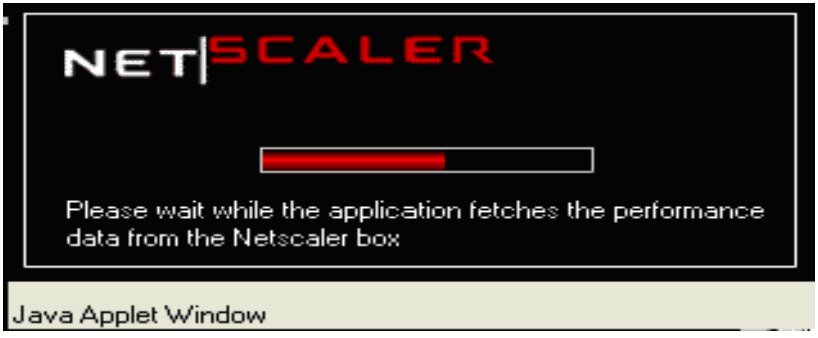
3. Click on the “Netscaler Statistical Utility” hyperlink to invoke Dashboard, the following window is displayed:

Figure 4-2 The NetScaler Login Page.



4. Enter the valid username and password in the corresponding fields that allow NetScaler 9000 system access (by default, the username is **`nsroot`** and the password is also **`nsroot`**), and then click Login button.
5. After authentication succeeds, the application shows the following wait message during the time NetScaler Dashboard fetches the real-time data for different reports from the NetScaler box it is monitoring. Please note that this message is shown only once during the launch of the application.

Figure 4-3 Application Load Message Box.



The following NetScaler Dashboard applet screen is displayed in your browser after the data is successfully fetched and processed:

Figure 4-4 The NetScaler Dashboard Screen.

4.3 Understanding Graphs and Legends

There are two different categories of Chart Types:

1. Fill Pattern: Bar, Stacked Bar, Area, Stacked Area and Pie chart types fall under this category;

   Hence the charts in the middle row shown in the image have Area and Bar chart types respectively. So the legend depicts the color chosen to fill / draw the plot area for its respective plot item.

2. Line Pattern: Line chart type (among those made available in Dashboard 5.0 to the user) falls under this category;

   The lines that are drawn using the plot points can have symbols (Circle, Diamond, Cross, Square, Rhombus etc. including NONE) to depict the plot points on a given plotted line. From the usability point of view it is helpful for the user to have symbols on the lines drawn to easily distinguish between data plot points and connector lines between two data plot points. The symbol shown in the legend painted with chosen color, is the symbol used on the drawn line to depict a plot point and the color used to fill symbol shape is the color used to show the respective plotted item.

4.4 Dashboard Components

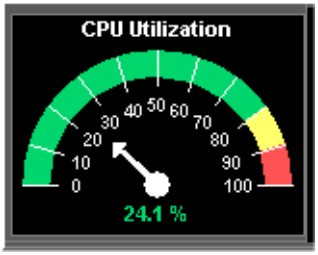
Dashboard consists of 7 main components (panels). They are:

- CPU Utilization Panel
- Memory Utilization Panel
- System Throughput Panel
- Requests Per Second Panel
- System Log Panel
- Global Statistics Panel
- Feature Statistics Panel

4.4.1 CPU Utilization Panel

The CPU Utilization panel reflects the NetScaler system's current CPU utilization as a percentage. The user can plot the CPU Utilization statistics in a graph.

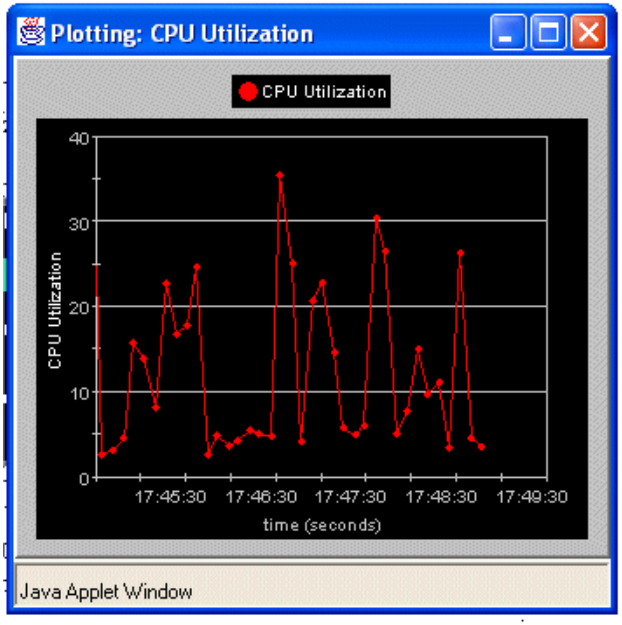
Figure 4-5 The CPU Utilization Panel.



To plot the CPU Utilization statistics in a graph/chart:

1. Right-click on the CPU Utilization Panel and select the “Plot…” option. The following chart is displayed:

Figure 4-6 Plotting chart for CPU Utilization.



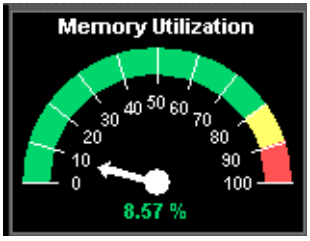
2. To change the chart type, right-click on the “Plotting: CPU Utilization” window and select the “Change Chart Type” option.
3. To show the grid lines on the chart, right-click on the Plotting chart and select the “Show Grid” option. To hide the grid lines on the chart, right-click on the Plotting chart and select the “Hide Grid” option.

4.4.2 Memory Utilization Panel

The Memory Utilization panel reflects NetScaler 9000 System's current memory utilization in the unit of percentage. When you move the cursor over Memory Utilization panel, the dashboard displays the memory used (in MB) and the total memory available for usage, in the following format:

<*Memory Used*> MB / <*Available Memory*> MB.

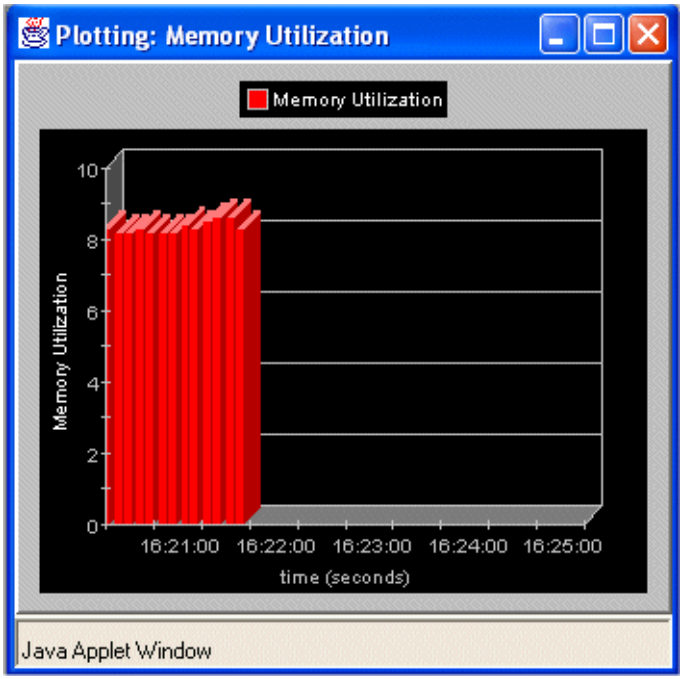
Figure 4-7 The Memory Utilization Panel.



To plot the Memory Utilization statistics in a graph/chart:

1. Right-click on the Memory Utilization Panel and select the "Plot…" option. The following chart is displayed:

Figure 4-8 Plotting chart for CPU Utilization.

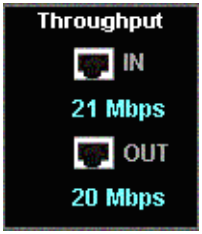


2. To change the chart type, right-click on the “Plotting: Memory Utilization” window and select the “Change Chart Type” option.
3. To show the grid lines on the chart, right-click on the Plotting chart and select the “Show Grid” option. To hide the grid lines on the chart, right-click on the Plotting chart and select the “Hide Grid” option.

4.4.3 System Throughput Panel

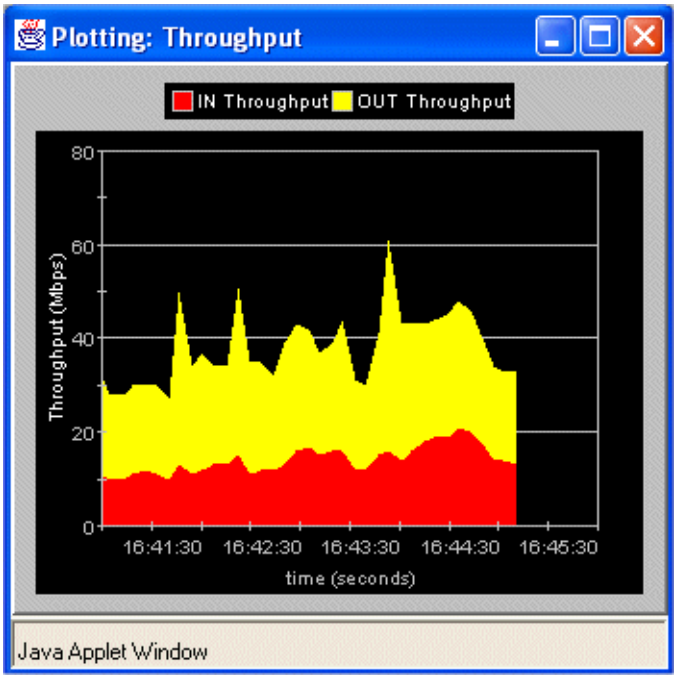
The System Throughput Panel depicts NetScaler 9000 system’s throughput in terms of incoming and outgoing traffic passing through the NetScaler 9000 system.

Figure 4-9 The System Throughput Panel.



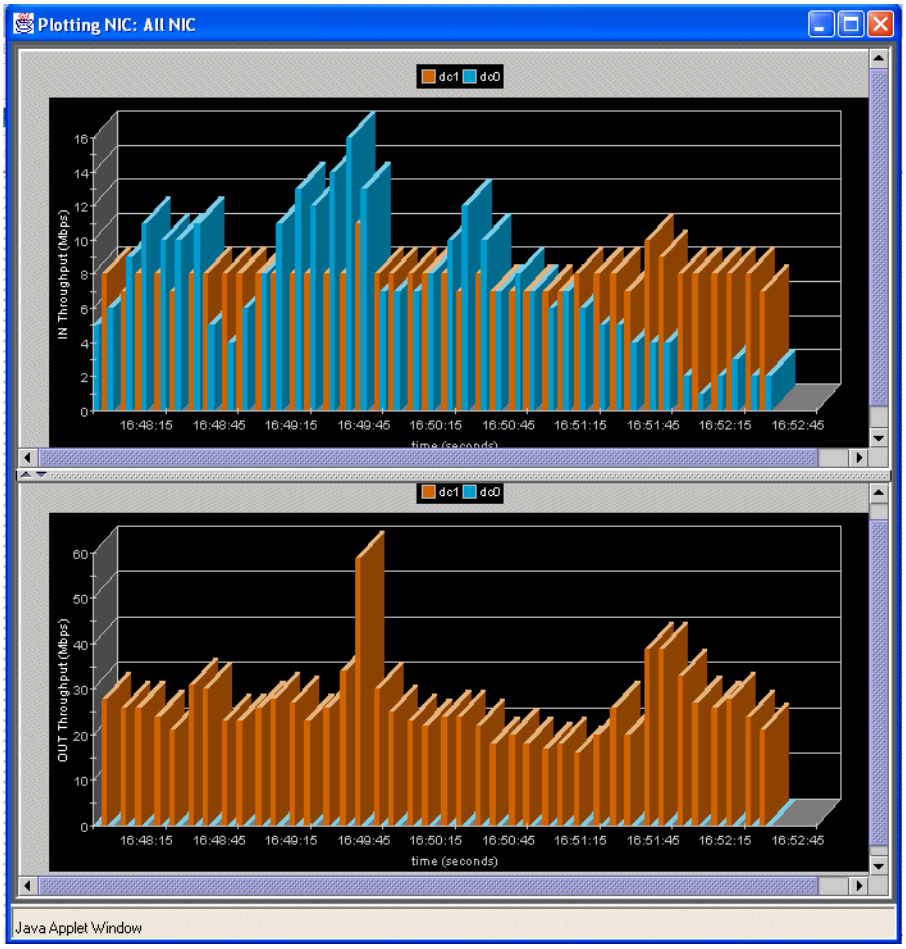
1. Right-click on the Throughput Panel and select the “Plot…” option. The following chart plots both the incoming throughput and outgoing throughput values

Figure 4-10 Plotting chart for System Throughput.



To view the comparative throughputs of all interfaces in NetScaler, right-click on the Throughput Panel and select the “Drilldown…” option. The following chart displays the comparative throughputs for each of the interface in NetScaler.

Figure 4-11 Plotting Chart that shows the comparative throughputs for each of the interface in NetScaler.



2. To change the chart type, right-click on the “Plotting: Throughput” window and select the “Change Chart Type” option.
3. To show the grid lines on the chart, right-click on the Plotting chart and select the “Show Grid” option. To hide the grid lines on the chart, right-click on the Plotting chart and select the “Hide Grid” option.

4.4.4 Requests per second Panel

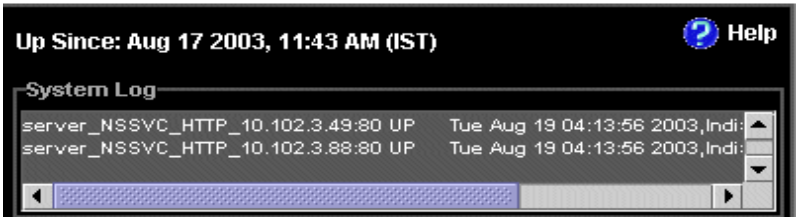
This panel reflects the current requests per second served by the NetScaler 9000 system.

Figure 4-12 The Requests per second Panel.

4.4.5 System Log Panel

The System Log panel displays all events logged in the system since the Dashboard was launched. The text on the top of this panel shows the timestamp since when the NetScaler system that is being monitored has been up and running.

Figure 4-13 The System Log Panel.


Up Since: Aug 17 2003, 11:43 AM (IST)
Help
System Log
server_NSSVC_HTTP_10.102.3.49:80 UP Tue Aug 19 04:13:56 2003,Indi:
server_NSSVC_HTTP_10.102.3.88:80 UP Tue Aug 19 04:13:56 2003,Indi:

Click on the Help button to launch Online Help system for the NetScaler Dashboard

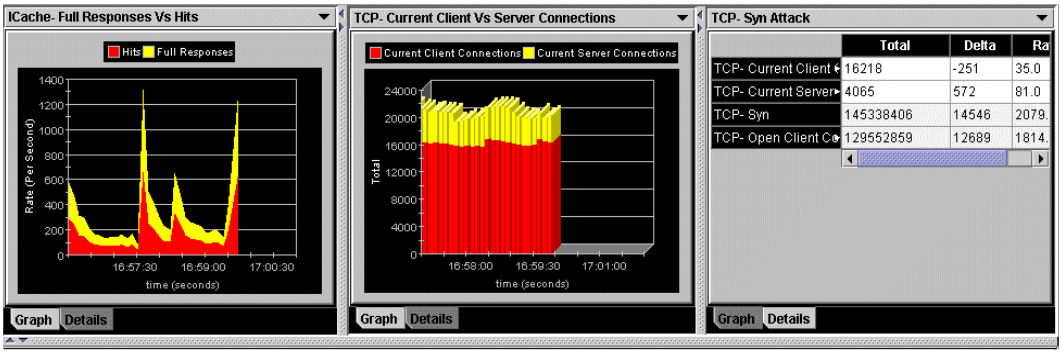
4.4.6 System Global Statistics Panel

The Global Statistics panel captures the NetScaler 9000 system's global statistics. These statistics are categorized into different groups, such as:

- HTTP
- TCP
- SSL
- ICache (Integrated Cache)

- Compression

Figure 4-14 The Global Statistics Panel.



1. To plot a statistic on the chart, click the drop-down list provided at the top of the Global Statistics Panel. Select the desired statistic. On selection, the chart plots the selected statistic. The "details" panel displays performance data of all the statistics falling under the parent group of the selected statistic.

   The meaning of the columns in the Details Panel is as follows:

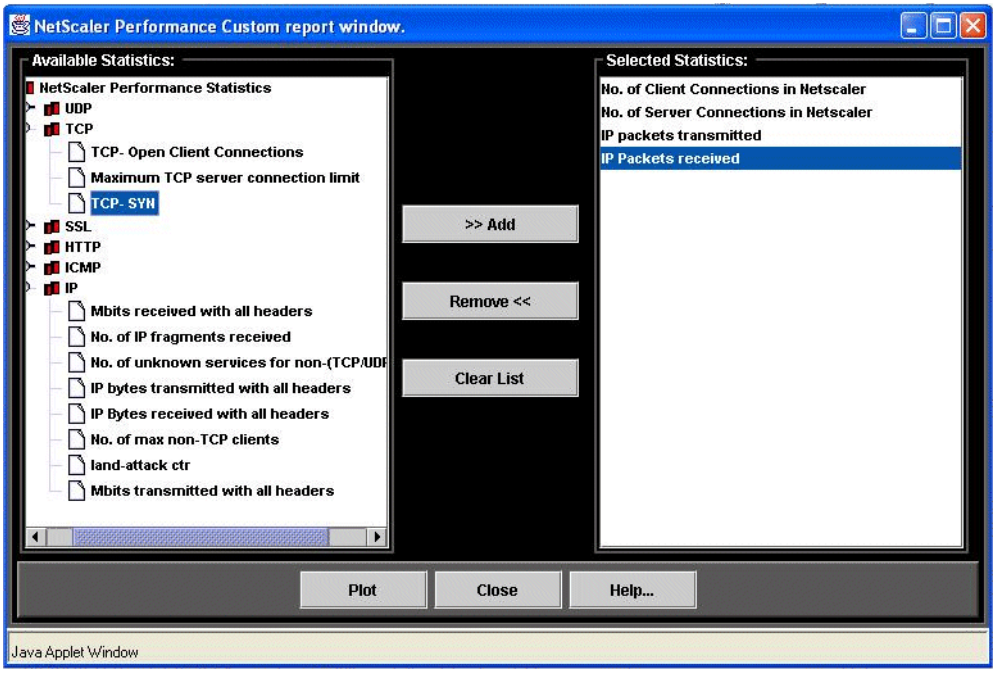
   - **`Total:`** Displays the cumulative total of the selected statistic.
   - **`Delta:`** Displays the recent changes in the statistic's value since the last refresh (usually since last 7 seconds).
   - **`Rate:`** Displays the statistic's rate per second.

2. To change the chart type, right-click on the Chart and select the "Change Chart Type" option. The chart types are Line, Bar, Area, Stacked Bar and Stacked Area.
3. To show the grid lines on the chart, right-click on the chart and select the "Show Grid" option. To hide the grid lines on the chart, right-click on the Plotting chart and select the "Hide Grid" option.
4. To change the value of units in the chart, right-click on the Chart and select the "Plot Statistic Unit" option. The supported units are Total, Delta and Rate.

Note: For certain statistics the unit selection may be disabled.

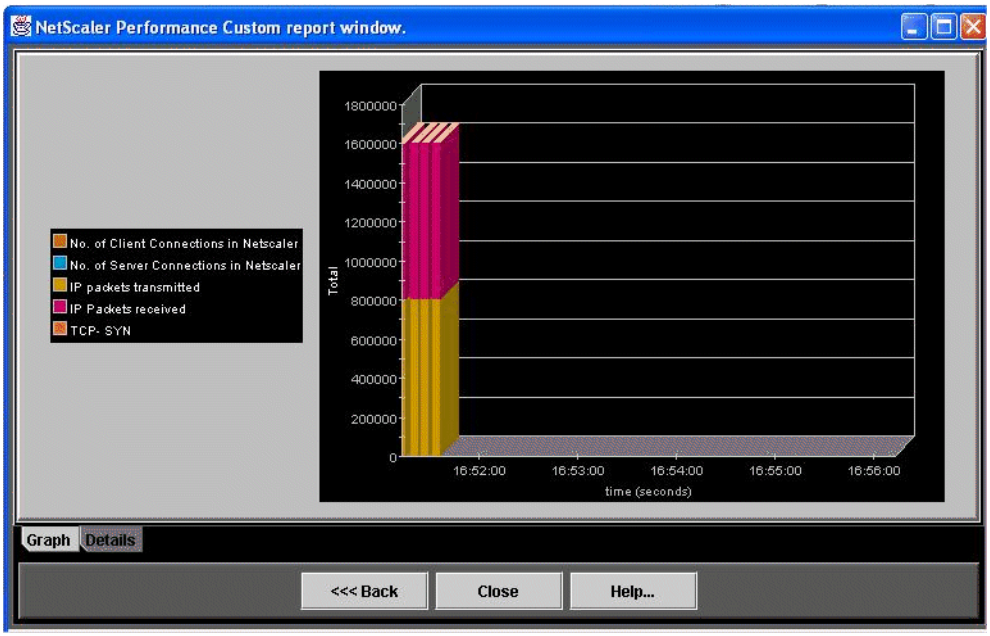
5. To generate a user-defined report, right-click on the Chart and select the "Custom Plot…" option. You would get a customized report window as shown in Figure 4-15.

Figure 4-15 NetScaler Performance Custom Report Window.



Here you can select at random and plot the global statistics categorized in different protocol / feature specific categories. The resulting window is shown in Figure 4-16:

Figure 4-16 NetScaler Performance Custom Report Window.



Compression Benefits

Compression statistics monitoring is categorized into 2 groups namely:

- **Content Compression:** The statistics in this category pertains only to those web resources that are successfully compressed by the Netscaler system. Examples of those objects are text files like HTML or ASP files.
- **Overall Compression:** The statistics in this category pertains to the entire web resources served by the Netscaler system. This includes resources that are successfully compressed by the system and those that may not be compressed. Some files like JPEGs, GIFs are already compressed and these may not be compressed again by the Netscaler system.

The following plots are available to monitor compression benefits

- **Compressible vs. Compressed data:** This graph belongs to “Content Compression” category and plots throughput of compressible data before and after compression. Supported units are Total, Delta and Rate.
- **UnCompressed vs. Overall Compressed Data:** This graph belongs to “Overall Compression” category and plots throughput of the overall

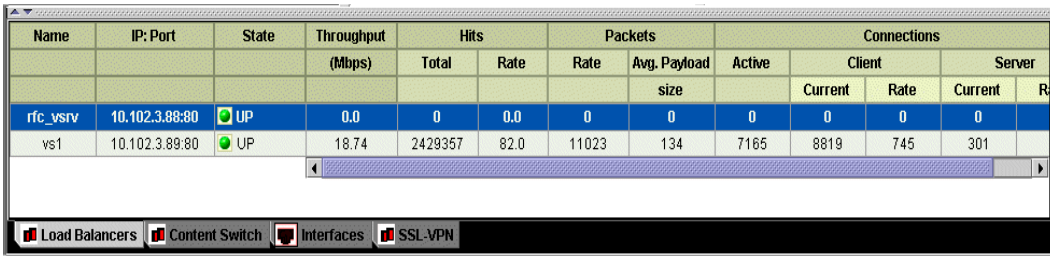
content served by the Netscaler system. Supported units are Total, Delta and Rate.

- **Content vs. Overall Compression Ratio(%):** This graph plots the benefits on content compression and overall compression in terms of percentage.

4.4.7 Feature Statistics Panel

The Feature Statistics Panel displays statistics belonging to the NetScaler's Key features, such as Load Balancing, Content Switching, Interfaces, SSL VPN etc. These statistics are displayed in a tabular format.

Figure 4-17 The Feature Statistics Panel.



4.5 Monitoring Performance Statistics of Key NetScaler Features

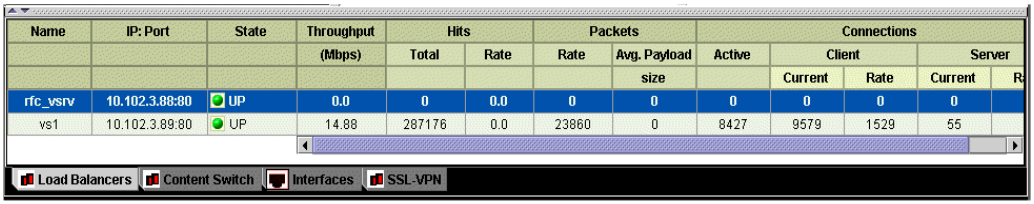
4.5.1 Load Balancing Virtual Servers

To view the performance information of Load balancers configured in Netscaler system:

1. Click the Load Balancers feature tab at the bottom of the panel.

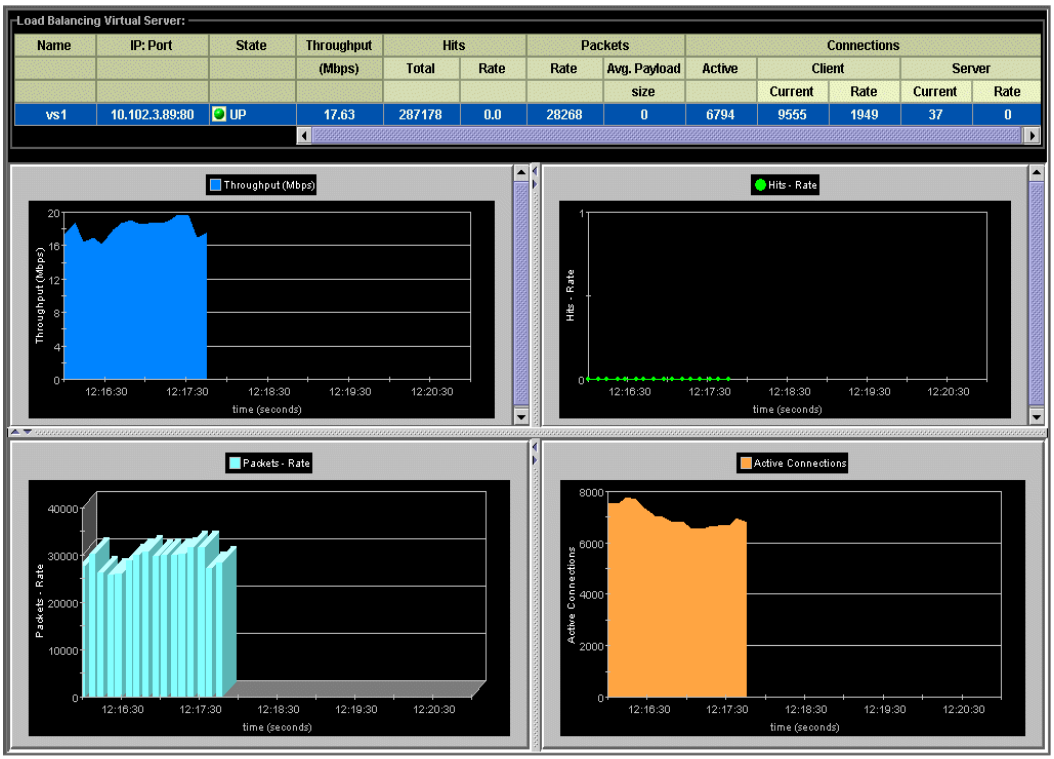
   The statistics of the configured Load Balancing Virtual Servers are displayed in a table as shown in Figure 4.18 below.

Figure 4-18 Load Balancing Statistics in a Tabular Form.



2. To plot the statistics displayed in the table, select the target row by left-clicking on it and then right click on the desired load balancing virtual server from the table and select the “Plot…” option. This action can also be achieved through double-clicking on the target row. The following chart is displayed plotting various statistics under this load balancing virtual server.

Figure 4-19 Performance statistics of a Load Balancing Virtual Server.



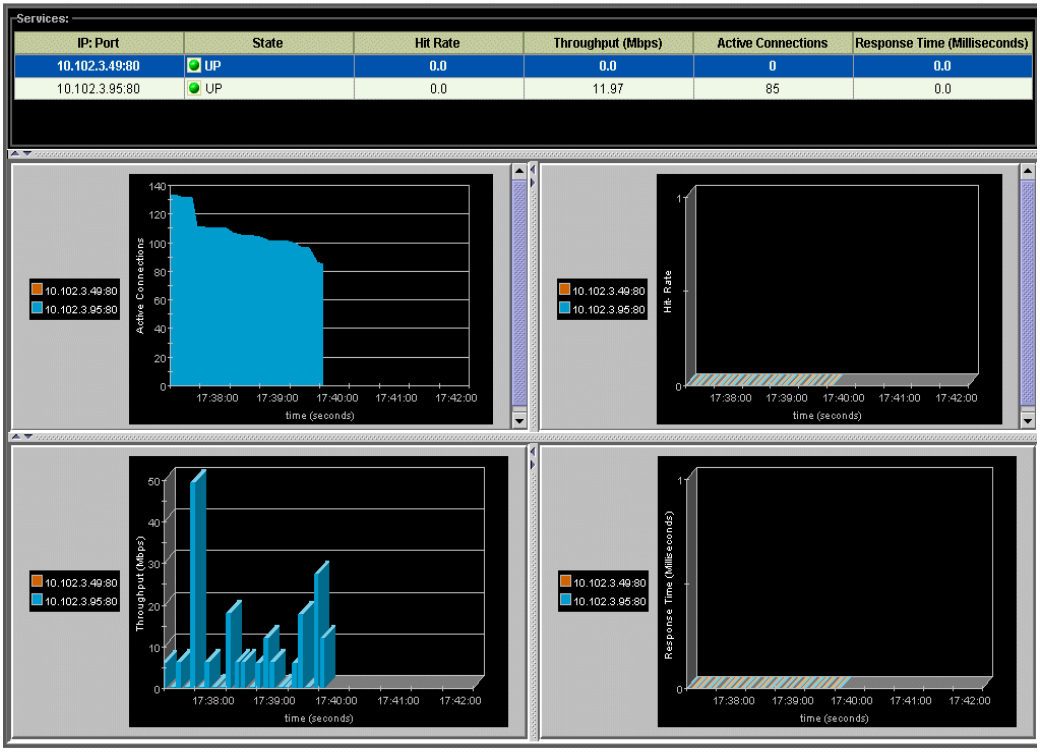
3. To plot services bound to a load balancing virtual server, select the target row by left-clicking on it and then right click on the desired load

balancing virtual server from the table and select the “Services…” option. The following chart is displayed plotting various statistics for all the services bound to this load balancing virtual server.

Note: An additional Pie chart type is available to view the distribution of the load over different services bound to the target Load balancing Virtual Server.

a. To further plot only a single service, select the target row by left-clicking on it and then right click on the desired service from the table and select the “Plot…” option. This action can also be achieved through double-clicking on the target row.

Figure 4-20 Performance statistics of the services associated to LB Virtual Server.

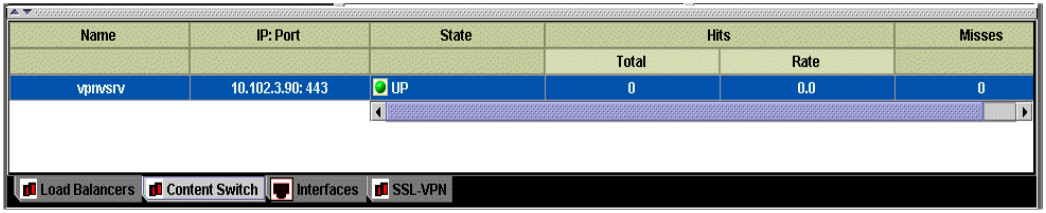


4.5.2 Content Switching Virtual Server

To view the performance information of Content Switching virtual servers configured in Netscaler system:

1. Click the Content Switch feature tab at the bottom of the panel. The statistics are displayed in a table as shown in Figure 4.21 below.

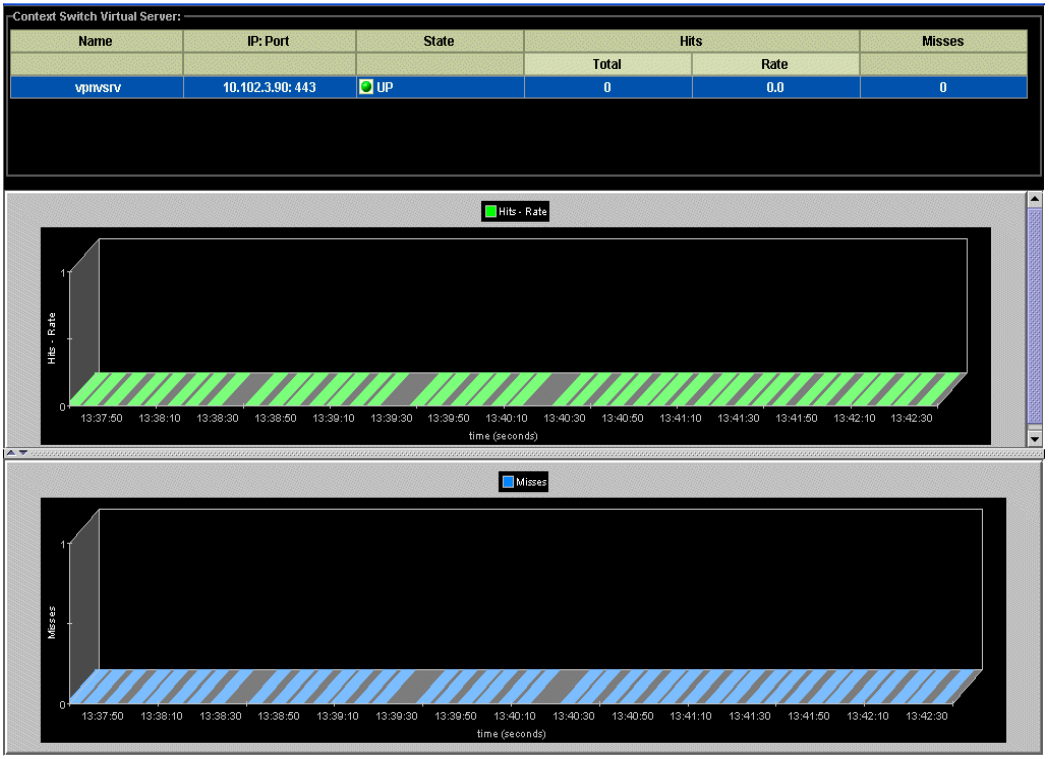
Figure 4-21 Content Switching Statistics in a Tabular Form.



Note: This table will display both content switching and cache redirection virtual servers configured in the Netscaler system

2. To plot the statistics displayed in the table, select the target row by left-clicking on it and then right click on the desired content switch virtual server from the table and select the “Plot…” option. This action can also be achieved through double-clicking on the target row. The following chart is displayed plotting various statistics under this content switching virtual server.

Figure 4-22 Performance statistics of a Content Switching Virtual Server.



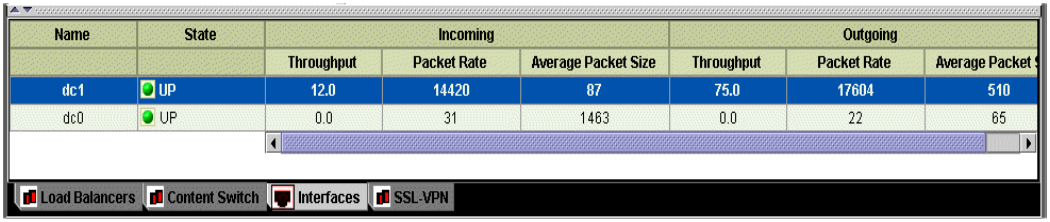
4.5.3 Network Interface Cards

To view the performance information of Interfaces configured in Netscaler system:

1. Click the Interfaces feature tab at the bottom of the panel.

The statistics of installed interfaces on NetScaler box are displayed in a table as shown in Figure 4.23 below.

Figure 4-23 NIC Statistics in a Tabular Form.



2. To plot the statistics displayed in the table, select the target row by left-clicking on it and then right-click on the desired Interface from the table and select the “Plot…” option. This action can also be achieved through double-clicking on the target row. The following chart is displayed plotting various statistics under this Interface

Figure 4-24 shows the Dashboard displaying the performance statistics of a NIC.

Figure 4-24 Performance statistics of a NIC.

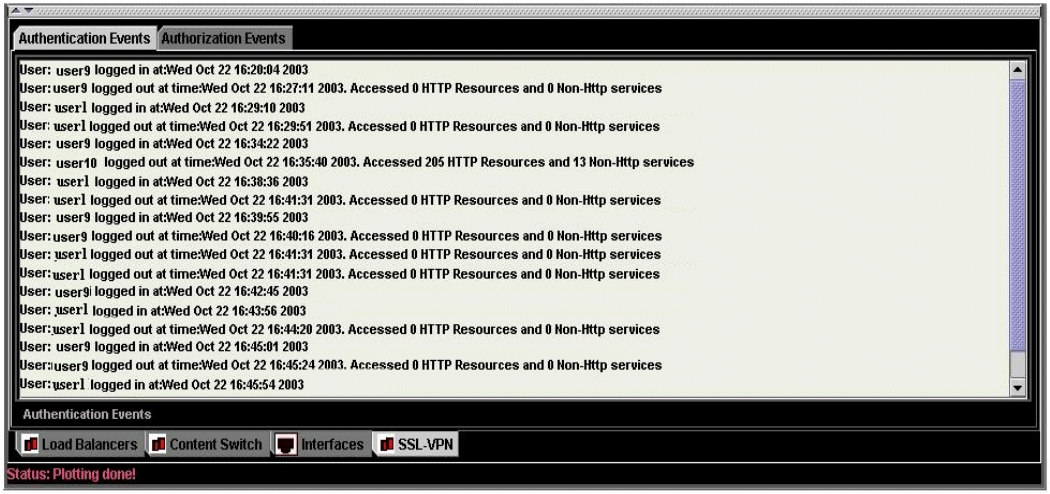
4.5.4 SSL VPN

To view the performance information of SSLVPN configured in Netscaler system:

1. Click the SSLVPN feature tab at the bottom of the panel.

   The SSLVPN member statistics, event logs and alerts are displayed as shown in the Figure 4.25 below.

Figure 4-25 Performance statistics of SSL VPN Feature.


Authentication Events
Authorization Events
User: user9 logged in at:Wed Oct 22 16:20:04 2003
User: user9 logged out at time:Wed Oct 22 16:27:11 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user1 logged in at:Wed Oct 22 16:29:10 2003
User: user1 logged out at time:Wed Oct 22 16:29:51 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user9 logged in at:Wed Oct 22 16:34:22 2003
User: user10 logged out at time:Wed Oct 22 16:35:40 2003. Accessed 205 HTTP Resources and 13 Non-Http services
User: user1 logged in at:Wed Oct 22 16:38:36 2003
User: user1 logged out at time:Wed Oct 22 16:41:31 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user9 logged in at:Wed Oct 22 16:39:55 2003
User: user9 logged out at time:Wed Oct 22 16:40:16 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user1 logged out at time:Wed Oct 22 16:41:31 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user1 logged out at time:Wed Oct 22 16:41:31 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user9i logged in at:Wed Oct 22 16:42:45 2003
User: user1 logged in at:Wed Oct 22 16:43:56 2003
User: user1 logged out at time:Wed Oct 22 16:44:20 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user9 logged in at:Wed Oct 22 16:45:01 2003
User: user9 logged out at time:Wed Oct 22 16:45:24 2003. Accessed 0 HTTP Resources and 0 Non-Http services
User: user1 logged in at:Wed Oct 22 16:45:54 2003
Authentication Events
Load Balancers
Content Switch
Interfaces
SSL-VPN
Status: Plotting done!

In Figure 4.25, the panel on the left side displays the various SSLVPN events. The “authentication events” pane displays the event logs of the user who logged In and Out of SSL VPN. The “authorization events” pane displays the Alerts of un-authorized access.

The panel on the right side plots the current numbers of sessions/users connected to the SSL VPN network. The details pane captures the other member statistics under SSLVPN.

Appendix A: Policy Expressions

Several NetScaler features are controlled using policies. For example, a compression policy defines the conditions for compressing content. A policy typically consists of an expression and an action. The following diagram illustrates this concept.

Figure A-26 Diagrammatic representation of a policy

The features that use policies are:

- Content Switching
- Content Filtering
- Compression
- Cache Redirection
- SSL VPN
- Priority Queuing
- DoS Protection
- Sure Connect TM

Expressions are a common pool of conditions that can be applied on content entering the NetScaler system. Expressions are shared among features. On the other hand, actions are feature-specific. For example, you can create an expression to identify ASP files. You can then create a compression policy that uses this expression to compress all ASP files. You can also create a content switching policy that redirects the request for an ASP file to an appropriate vserver. The following example illustrates this.

Example

```
add expression ext_asp "URL == /*.asp"

add cmp policy cmp_asp -rule ext_asp -resAction COMPRESS

add cs policy cs_asp -rule ext_asp
```

Notice that the commands to create the compression and content switching policies invoked identical expressions but different actions.

A.1 Understanding Expressions

Expressions are the most fundamental components of a policy. It represents a single condition that is evaluated against an HTTP request (or in some cases, such as caching and compression, against the HTTP response). You can create a simple expression to check for conditions such as:

- File types
- Length of a URL
- Contents of the host header
- Browser type

The following examples illustrate the creation of expressions using the add expression command.

```
add expression gif_file "URL == /*.gif"

add expression url_len "URLLEN > 5"

add expression has_cookie "HEADER Cookie EXISTS"

add expression browser_mozilla "HEADER User-Agent
CONTAINS Mozilla"
```

You can also combine expressions to create compound expressions.

```
add expression image_file "gif_file || URL == *.jpeg ||
URL == *.jpg"
```

A.1.1 Components of an Expressions

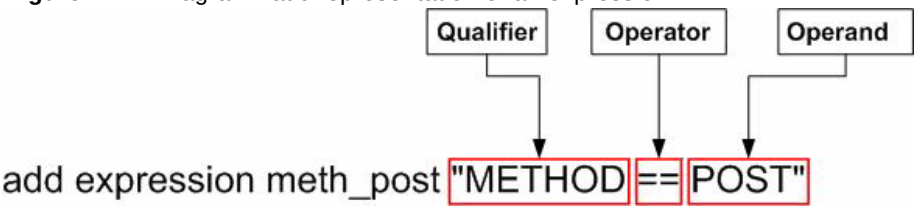
Expressions consist of the following components:

- **Qualifier:** The qualifier represents the information within a request that needs to be tested. The HTTP method, URL, and length of a URL are examples of qualifiers.

- **Operators:** Operators identify the operation that an object performs on its operands.
- **Operand:** Operands define the values of the corresponding qualifiers.

The components of an expression are illustrated as follows.

Figure A-27 Diagrammatic representation of an expression



Note: For unary operators like EXISTS, NOTEXISTS and CONTENTS, no operand should be given.

The following sections cover these components in detail.

A.1.1.1 Understanding Qualifiers

As mentioned earlier, the qualifier represents the information within a request that needs to be tested. Qualifiers are generally components of HTTP requests and headers.

The generalized format for specifying the qualifiers in expressions is:

`[<flow-type>.<protocol>.]qualifier`

Where flow-type can be either REQUEST or RESPONSE and protocol can be HTTP, TCP or IP.

The following examples illustrate this format.

Example

`REQUEST.HTTP.URL`

In this example, the qualifier tests the contents of a URL.

The commonly used qualifiers are:

- **`METHOD`**: This qualifier deals with the HTTP request method, in general GET and POST, although all HTTP/1.1 standard headers are accepted for expressions (but not extensions such as the WebDAV method ìSEARCHî).

Example:

```
add policy expression meth_get "METHOD == GET"
```

An alternate form of this expression is as follows.

```
add policy expression meth_get "REQ.HTTP.METHOD == GET"
```

- **URL**: This qualifier deals with the URL in a HTTP header. This does not include the query string (i.e. any characters following the ? when present).

```
add policy expression url_html "URL == /*.html"
```

An alternate form of this expression is as follows.

```
add policy expression url_html " REQ.HTTP.URL ".
```

- ⟨**URLTOKENS**: This qualifier deals with special tokens in the URL. This allows an expression to detect if any special tokens are contained within the full URL. For more information on URL Tokens, see *NetScaler 9000 Series Command Reference*.
- ⟨**VERSION**: This qualifier deals with the HTTP request version. There is special significance to the fact that many web servers will answer a request when no version identifier is specified in the HTTP request. The format for the version is `HTTP/X.X` where `X` is an integer.

```
add policy expression http_1_0 "VERSION == HTTP/1.0"
```

An alternate form of this expression is as follows.

```
add policy expression http_1_0 " REQ.HTTP.VERSION"
```

- ⟨**HEADER**: This qualifier is same as qualifier **HTTPHEADER.** This qualifier specifies a given HTTP header by name. The header does not have to be any of the standard headers, but can match a plain-text string. If there are more than one instances of a particular header, the Netscaler policy engine will only test against the last HTTP header of the name specified. This could cause problems if standard browsers, for example, start issuing distinct cookies in separate cookie headers.

```
add policy expression host_hdr "HEADER Host CONTAINS
mydomain.com"
```

An alternate form of this expression is as follows.

```
add policy expression host_hdr " REQ.HTTP.HEADER"
```

- ⟨**URLQUERY**: This qualifier matches against the query portion of a URL (i.e. after the ?).

An alternate form of this expression is as follows.

REQ.HTTP.URLQUERY.

- ⟨**URLLEN**: This qualifier specifies the total length of the URL as a whole. Example:

```
add policy expression long_url "URLLEN > 250"
```

An alternate form of this expression is as follows.

```
add policy expression long_url "REQ.HTTP.URLLEN"
```

- ⟨**QUERYLEN**: This qualifier specifies the length of the query alone (not including the path of the URL).

An alternate form of this expression is as follows.

REQ.HTTP.URLQUERYLEN.

- ⟨**SOURCEIP**: This qualifier specifies the client's IP address (or range with netmask).

```
add policy expression cli_ip "SOURCEIP == 192.168.13.68"
```

An alternate form of this expression is as follows.

```
add policy expression cli_ip ìREQ.IP.SOURCEIPî
```

- ⟨**DESTIP**: This qualifier indicates the target IP address, usually the vserver's IP address.

```
add policy expression vpn_ip "DESTIP == 210.18.13.5"
```

An alternate form of this expression is as follows.

```
add policy expression vpn_ip " REQ.IP.DESTIP"
```

- ⟨**SOURCEPORT**: This qualifier specifies the client's TCP port number (or range):

```
add policy expression user_ports "SOURCEPORT ==
1024-65535"
```

An alternate form of this expression is as follows.

```
add policy expression user_ports "REQ.TCP.SOURCEPORT"
```

- ⟨**DESTPORT**: This qualifier specifies the target TCP port

```
add policy expression vpnport "DESTPORT == 443"
```

An alternate form of this expression is as follows.

```
add policy expression vpnport "REQ.TCP.DESTPORT"
```

A.1.1.2 Understanding Operands

An operand defines the values for the corresponding qualifiers. Consider the following example.

```
add expression exp_gif "url == *gif"
```

The “*” wildcard character can be used to match the string within the specified qualifier. This character can appear only once within the string. By using wildcard characters, the user can restrict the processing of a string. For example, in a string “/*gif” and “gif” will match on the first instance of gif, but not at the last instance of gif if there is more than one gif in the string. This can be of particular importance when using rule based persistence, so the user has to carefully craft the strings that should be matched.

A.1.1.3 Understanding Operators

An operator identifies an operation an object performs on its operands. Particular qualifiers will limit what operators are available. Table I-1 provides a brief description of each operator.

Table 0-1. Operators

Operator	Description
==, !=, EQ, NEQ Note: With == or EQ operators,	These operators test for exact matches, but in doing so, are case sensitive. These operators are useful for creating permissions to allow particular strings when they must meet an exact syntax, but exclude other strings. "cmd.exe" is NOT EQUAL to "cMd.exe".
GT	This operator is used for numerical comparisons and is used on the length of the URLs and query strings.
CONTAINS, NOTCONTAINS	These operator perform check against the specified qualifier to determine if the specified string is contained in the qualifier. These operator are not case sensitive.

Table 0-1. Operators

Operator	Description
EXIST, NOTEXISTS	These operators check for the existence of particular qualifier. For example, these operators can be applied to HTTP headers to determine if a particular HTTP header exists, or if the URL Query exists.
CONTENTS	This operator checks if the qualifier exists and if it has contents (i.e. if a header exists, and has a value associated with it, no matter what the value).

A.1.2 Using Expressions

Expressions are categorized as:

- Simple Expressions
- Compound Expressions
- Response Side Expressions

A.1.2.1 Using Simple Expressions

Simple expressions, as the name implies, check for a single condition. Examples of simple expressions are as follows:

```
add policy expression meth_trace "METHOD == TRACE"

add policy expression url_cgi "URL == /cgi-bin/*"

add policy expression exp_images "URL CONTAINS /images/"

add policy expression jsession_url "URL CONTAINS
jsessionid= -length 8"

add policy expression cookie_monster "HEADER Cookie
CONTAINS 'monster=true'"

add policy expression no_hdr_host "HEADER Host NOTEXISTS"

add policy expression rfc1918_10 "SOURCEIP == 10.0.0.0
-netmask 255.0.0.0"

add policy expression rfc1918_172_16 "SOURCEIP ==
172.16.0.0 -netmask 255.240.0.0"
```

```
add policy expression rfc1918_192_168 "SOURCEIP ==
192.168.0.0 -netmask 255.255.0.0"
```

A.1.2.2 Using Compound Expressions

Compound expressions check for multiple conditions. Expression logic is formed with one or more expression names logically connected using the logical operators && and ||, and are grouped for order of evaluation using the symbols (and). Processing of compound expressions is done from left to right, and is done with "lazy" evaluation, i.e. once the final result is known, evaluation is terminated. For examples of how this can impact compound expression creation, see rule based persistence in the section Length and Offset Expressions.

Compound expressions can be categorized as:

- Named Compound Expressions
- Inline Compound Expressions

Named compound expressions are independent entities. A named compound expression can be reused by other policies. Use the "add policy expression" command to create a named compound expression.

The same expression logic is used in various other commands with the -rule, -reqRule, or -respRule parameters.

Example 1

Test true if a request is not a GET, POST, or HEAD request:

```
add policy expression not_get "METHOD != GET"
```

```
add policy expression not_post "METHOD != POST"
```

```
add policy expression not_head "METHOD != HEAD"
```

```
add policy expression not_normal_method "not_get &&
not_post && not_head"
```

or simply by using inline expressions:

```
add policy expression not_normal_method "METHOD != GET &&
METHOD != POST && METHOD != HEAD"
```

or by using a combination of inline expressions and expression names:

```
add policy expression not_post "METHOD != POST"
```

```
add policy expression not_normal_method "METHOD != GET &&
not_post && METHOD != HEAD"
```

Example 2

Test true if the request does not have normal headers:

```
add policy expression no_hdr_host "HEADER Host NOTEXISTS"
```

```
add policy expression no_hdr_user_agent "HEADER
User-Agent NOTEXISTS"
```

```
add policy expression not_normal_hdrs "no_hdr_host &&
no_hdr_user_agent"
```

Example 3

Combine the two into an expression that uses both of these compound expressions

```
add policy expression bad_request "not_normal_method ||
not_normal_hdrs"
```

To use this expression with content filtering to deliver a page “400 Bad Request” with errorcode 400, the following would be added to complete the configuration:

```
add filter action bad_reqact errorcode 400 "400 Bad
Request"
```

```
add filter policy block_bad_requests -rule "bad_request"
-reqAction bad_reqact
```

Alternatively, it could be written as follows to avoid creating named compound expressions:

```
add filter policy block_bad_requests -rule "(not_get &&
not_post && not_head) || (no_hdr_host &&
no_hdr_user_agent)" -reqAction bad_request
```

Alternatively, it could be written as follows to avoid creating named expressions:

```
add filter policy block_bad_requests -rule "(METHOD !=
GET && METHOD != POST && METHOD != HEAD) || (HEADER Host
NOTEXISTS && HEADER User-Agent NOTEXISTS)" -reqAction
bad_request
```

To activate this filter policy for all the http requests, it should be bound globally:

```
bind filter global block_bad_requests
```

A.1.2.3 Using Response Side Expressions

By default, all the expressions are evaluated only for requests. In 6.0, the expressions which can be evaluated at response time are also supported.

To specify the expression which must be evaluated at the response time, qualifier must be qualified with response flow-type and appropriate protocol for that qualifier. For example, qualifier RES.HTTP.HEADER should be used to make use of response http header in expressions. When qualifier is given in the old format, the default values for flow-type and protocol are taken for that qualifier. For each qualifier, only certain valid combinations of flow-type and protocol are accepted, e.g. only REQUEST flow-type and HTTP protocol combination is valid for URL qualifier, since these are default values too, qualifiers URL in old format is same as qualifier REQ.HTTP.URL in new format.

Below table summarizes all the qualifiers with valid values of qualifiers and their default values:

Figure A-28 Qualifiers with valid values

	Qualified as request	**Qualified as Response**	**Default**
VERSION	REQ.HTTP.VERSION	RES.HTTP.VERSION	REQ.HTTP.VERSION
METHOD	REQ.HTTP.METHOD	No	REQ.HTTP.METHOD

Figure A-28 Qualifiers with valid values

	Qualified as request	**Qualified as Response**	**Default**
URL URLSUFFIX URLTOKENS URLQUERY URLLEN URLQUERYLEN	REQ.HTTP.URL REQ.HTTP.URLSUFFIX REQ.HTTP.URLTOKENS REQ.HTTP.URLQUERY REQ.HTTP.URLLEN REQ.HTTP.URLQUERYLEN	No	REQ.HTTP.URL REQ.HTTP.URLSUFFIX REQ.HTTP.URLTOKENS REQ.HTTP.URLQUERY REQ.HTTP.URLLEN REQ.HTTP.URLQUERYLEN
HEADER/ HTTPHEADER	REQ.HTTP.HEADER	RES.HTTP.HEADER	REQ.HTTP.HEADER
SOURCEIP DESTIP	REQ.IP.SOURCEIP REQ.IP.DESTIP	RES.IP.SOURCEIP RES.IP.DESTIP	REQ.IP.SOURCEIP REQ.IP.DESTIP
SOURCEPORT DESTPORT	REQ.TCP.SOURCEPORT REQ.TCP.DESTPORT	RES.TCP.SOURCEPORT RES.TCP.DESTPORT	REQ.TCP.SOURCEPORT REQ.TCP.DESTPORT
VPNSERVICE VPNPORT (Deprecated)	REQ.IP.DESTIP REQ.TCP.DESTPORT	No	REQ.IP.DESTIP REQ.TCP.DESTPORT
LOCATION	NO	NO	LOCATION
COMPOUND	Deprecated	Deprecated	N/A

Now, expressions can take more general form in which request as well as response flow type qualifiers are combined within a compound expression:

Example

```
add expression txt_url "url == *.txt"
```

```
add expression can_compress "header user-agent contains
‘Internet Explorer’ && (txt_url || res.http.header
content-encoding == text/html)"
```

A.1.2.4 White space and escape sequences in operand string

While specifying the rules in policies (or expressions in add policy expression), if white space characters (space or tab) or escape sequences

```
add cs policy cs_pol1 -rule "url CONTAINS sports ||
http_port || (HEADER Cookie contains ’abc pqr
```

or

```
add cs policy cs_pol1 -rule "url CONTAINS sports ||
http_port || (HEADER Cookie contains \"abc pqr
```

or

```
add cs policy cs_pol1 -rule "url CONTAINS sports ||
http_port || (HEADER Cookie contains \’abc pqr
```

To specify double quotes/single quotes within rule string (or expression), triple escaped quotes (\\” or \\’) should be used. Below are examples:

```
add cs policy cs_pol2 -rule "url contains ’a \\"b\\"
\\’c\\’ d’"
```

or

```
add cs policy cs_pol2 -rule "url contains \"a \\"b\\"
\\'c\\\' d\""
```

or

```
add cs policy cs_pol2 -rule "url contains \’a \\"b\\"
\\’c\\’ d\’"
```

A.1.3 Length and Offset Expressions

Length and Offset parameters are used in expressions that are configured for either making the load balancing decisions, or with persistence. For example, the load balancing algorithm is set to token, or the persistence is set to any of rule, urlPassive or customerServerID.

When any expression is evaluated as being true, it returns a pointer to a buffer that contains the content and is then used with any of the rule controlled activities. Table I-2 defines the default behavior of what the buffer contains for combinations of qualifier and operator:

Table 0-2. Combination of qualifiers and operators and contents of the resultant buffer

Qualifier and Operator	Buffer Contains
URL CONTAINS	Data from the point where the string matches to the end of URL.
URL CONTENTS	The entire URL.
HEADER CONTAINS	Data from the point where the string matches to EOL.
HEADER CONTENTS	The entire header, including the header name.
URLQUERY CONTAINS URLQUERY CONTENTS	Data from the point where the string matches. The entire query, excluding the ? and trailing white space.

The length and offset parameter are then applied to the default buffer. All other expression data is considered undefined, and should be set to NULL even in the case of a TRUE evaluation. The evaluation on compound expressions is done in a lazy way, so given the expression (true || false || true), the buffer will be returned from the first expression, even though the last expression would also evaluated as true. Given the expression ((true && true) || true), the buffer value from the second expression would be returned. Finally, given the following expressions:

```
add policy expression jsession_url "URL CONTAINS
jsessionid= -length 6 –offset 2"

add policy expression jsession_query "URLQUERY CONTAINS
jsessionid= -length 6 –offset 2"

add policy expression jsession_cookie "HEADER Cookie
CONTAINS jsessionid -length 6 –offset 2"
```

```
add policy expression sess "jsession_cookie ||
jsession_query || jsession_url"
```

For example, if a request contains the following:

```
GET /test.jsp;jsessionid=123456789?jsessionid=zyxwvutsr
HTTP/1.0


Cookie: jsessionid=abcdefghi
```

For the above request, the buffer used for further decision making would contain the value cdefgh. If the cookie was missing, the buffer would contain the value xwvuts.

If the above expression was specified for token based load balancing and if the compound expression evaluated as true, the buffer would be hashed to create an index into the appropriate vserver service pool, and the request would be directed to that server pool. If the rule evaluated as false, a default load balancing metric of round robin would be used.

If this expression was specified for rule based persistence and if the rule tests true, the value in the buffer will be used to create a persistent session entry, which will then be associated with the server selected using the load balancing algorithm. If the rule tests false, then the session will be load balanced with no persistence.

When URL Passive and Custom Server ID persistence is used, the behavior is basically the same, except the nature of the value that is expected is different. In URL Passive, the buffer should contain a value that is equivalent to the hexadecimal IP address and port of the service that the session should be bound to. In the case of a custom server ID, the buffer is expected to contain a numerical value that is assigned to a service through the parameter –serverid in either add service or set service commands.

A.1 Using an expression in a policy definition

Policies are generally in the form : "add <policytype> policy –rule <expression> …". A rule is nothing but an expression used in a policy. Here, expression logic can also be directly specified in expression without having to create a named expression. Examples are:

```
add filter policy filter_nonget –rule "method != get"
–reqAction RESET
```

```
add filter policy filter_nongetpost –rule "method != get
&& method != post" –reqAction RESET
```

Policies can also use a combination of named expressions and expression logic too. One such example is:

```
add expr http_port "destport == 80"

add expression excel_ppt "RES.HTTP.HEADER Content-Type
CONTAINS application/vnd.ms-excel || RES.HTTP.HEADER
Content-Type CONTAINS application/vnd.ms-powerpoint"

add cmp policy cmppol –rule "(sourceip == 10.102.0.0
–netmask 255.255.0.0 && http_port) || excel_ppt"
–resAction COMPRESS
```

In above examples, filter policy and compression policies use built-in actions RESET and COMPRESS.

Expression_logic can be described by below grammar:

```
<qualifier> := <basic-qualifier>

:= <flow-type>.<protocol>.<basic-qualifier>


<simple-expr> :=  <non-ip-header-qualifier> <binary-op>
<operand>

:=  <non-ip-header-qualifier> <unary-op>

:=  <header-qualifier> <header-name> <binary-op>
<operand>

:=  <header-qualifier> <header-name> <unary-op>


<simple-expression> := <simple-expr>

:=  <simple-expr> -length <length>

:=  <simple-expr> -length <length> -offset <offset>

:=  <ip-qualifier> <binary-op> <ipaddr>

:=  <ip-qualifier> <binary-op> <masked-ipaddr> -netmask
<netmask>


<compound-expression> := <simple-expression>

:= <expression-name>
```

:= (<compound-expression>)

:= <compound-expression> && <compound-expression>

:= <compound-expression> || <compound-expression>

Here, for <header-qualifier> basic qualifier is HEADER while for <ip-qualifier>, basic qualifiers are SOURCEIP or DESTIP (previously VPNSERVICE), rest of the qualifiers are <non-ip-header-qualifier>. CONTENTS, EXISTS and NOTEXISTS are the only unary operators (<unary-op>), rest of the operators are binary.

Appendix B: NetScaler API Reference

This chapter provides information on the NetScaler Application Programming Interface (API) and detailed instructions on how to use the API to implement customized client applications.

This section contains the following topics:

- Introducing NetScaler Application Programming Interface
- Benefits of NetScaler API
- Hardware and Software Requirements
- Interface Description
- NetScaler API Architecture
- The NSConfig Interface
- Example: Setting the NetScaler Configuration
- Example: Querying the NetScaler Configuration
- The Web Service Definition Language (WSDL)
- Creating Client Applications using the NSConfig.wsdl File
- Securing NetScaler API Access

This section is intended for developers and administrators who will be using the NetScaler API to implement customized client applications.

B.1 Introducing NetScaler Application Programming Interface

The NetScaler 9000 system can be configured using an external Application Programming Interface (API). The NetScaler API allows programmatic communications between client applications and the NetScaler 9000 system. This interface provides the means for a custom client application to configure and monitor the state of the NetScaler 9000 system.

The NetScaler API is based on the Simple Object Access Protocol (SOAP) over HTTP and is used to develop custom client application that will configure and monitor the NetScaler 9000 system. SOAP is a transport protocol for exchanging information in a decentralized, distributed environment and enables you to write the business logic and schema for facilitating business-to-business transactions over the Internet.

B.2 Benefits of NetScaler API

The following are the benefits of the NetScaler API:

- The NetScaler API provides developers the advantage of controlling the NetScaler 9000 system from a custom application. The API enables the client application to configure and monitor the NetScaler 9000 system.
- The NetScaler interface allows the developers to easily and quickly develop client applications using a language and platform with which the developer is comfortable.
- The NetScaler API provides a secure, end-to-end, standards-based framework that integrates into the existing infrastructure.

B.3 Hardware and Software Requirements

To work with the NetScaler API, your system needs to meet the following hardware and software setup and requirements:

- A client workstation
- Access to a NetScaler 9000 system (version 5.0 or higher).
- A SOAP client tool kit (supporting SOAP version 1.1 and above) and the development environment for the tool kit (for example, if you use a Visual Basic tool kit, you must have Visual Basic installed on your system).

B.4 Interface Description

The NetScaler API consists of the `NSConfig` interface. The `NSConfig` interface includes methods for setting and querying the NetScaler configuration. These methods allow the client application using the `NSConfig` interface to perform almost all operations that an administrator would normally perform with the NetScaler CLI or GUI.

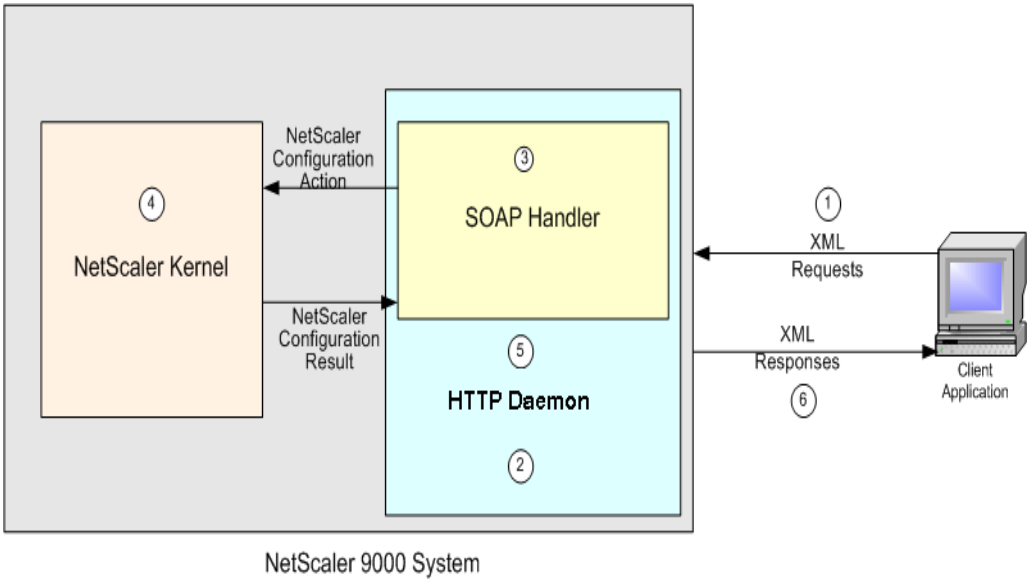
NetScaler provides an interface description using the Web Services Definition Language (WSDL) that facilitates the development of client applications using a language and platform of the developer's choice.

B.5 NetScaler API Architecture

The NetScaler API architecture is designed to allow **NSConfig** client requests to be routed through HTTP daemon, running on the target NetScaler system, to a SOAP handler that translates the SOAP request into a call to the (internal) NetScaler kernel configuration API.

Figure B-1 illustrates the NetScaler API Architecture.

Figure B-1 : The NetScaler API Architecture.



The following steps explain the NetScaler API Architecture:

1. The client formats a request containing XML conforming to the SOAP protocol and sends it to NetScaler 9000 system.
2. The HTTPD server instance on the NetScaler 9000 system routes this request to a SOAP handler.
3. The SOAP handler interprets the SOAP headers, and maps the enclosed request to an internal NetScaler configuration function.

4. The NetScaler kernel acts on the request and returns one or more responses.
5. The SOAP handler then translates the response(s) to a SOAP response message.
6. The XML response is then sent back to the client in a HTTP response.

B.6 The NSConfig Interface

The `NSConfig` interface closely mirrors the structure of the NetScaler 9000 system's Command Line Interface (CLI). The administrators and programmers who are familiar with the NetScaler 9000 system's CLI can easily create and implement custom applications to query or set the NetScaler 9000 system configuration. This semantic and syntactic closeness between the API and the CLI helps in leveraging the familiarity and expertise that has been gained using the two interfaces.

The `NSConfig` interface contains a method corresponding to each CLI command.

Note:

There are several CLI commands which are not included in the API, and a few instances where the method name and the CLI command differ.

Refer to the <*portType*> section of the WSDL for a complete list of methods and their names.

Let us take the example of **add lb vserver** CLI command for creating a load balancing virtual server. The following is the CLI command:

add lb vserver <*vServerName*> <*serviceType*> [<*IPAddress*> <*port*>]

where:

serviceType = (HTTP | FTP | TCP | UDP)

The corresponding API call, in the C language, would be:

```
int ns__addlbvserver(void *handle,
                     string vServerName,
                     string serviceType,
                     string IPAddress,
                     unsignedShort port,
                    ns__addlbvserverResponse *out);
```

Note: The exact syntax of the API call will depend on the language being used to write the client program. The above `ns__addlbvserver` function prototype is similar to the one that would be generated by the gSOAP package at `http://www.cs.fsu.edu/~engelen/soap.html`.

The result that is returned for all `NSConfig` requests consists of:

- **rc:** An integer return code. The value is zero if the request succeeded; a non-zero value is returned if the request failed.
- **message:** A string message. This contains meaningful information only if the request fails (rc is non-zero). For example, “Required argument missing”.
- **List:** A type-specific list of result entities. This element is present only for requests that retrieve information from the NetScaler 9000 system. For example, the API method names starting with “`get`”, which corresponds to the CLI show commands.

B.7 Example: Setting the NetScaler Configuration

This example shows a NetScaler CLI command, the corresponding API method, the resulting XML request, and the XML response that will be sent back to the client.

Note: The actual API method and the XML SOAP message contents may differ from the example shown below. The XML shown will be encased in a SOAP envelope, which will in turn be carried in an

HTTP message. For more information on this, see http://www.w3.org/TR/SOAP.

The following is the CLI command to create a Load Balancing virtual server:

```
add lb vserver vipLB1 HTTP 10.100.101.1 80
```

The following is the corresponding API method for the above CLI command:

```
ns__addlbvserver (handle, “vipLB1”, “HTTP”,
“10.100.101.1”, 80, &out);
```

The request XML generated for this request would be:

```
<ns:addlbvserver>
<vServerName xsi:type="xsd:string" >vipLB1</vServerName>
<serviceType xsi:type="ns:vservicetypeEnum>HTTP</
serviceType>
<IPAddress xsi:type="xsd:string">10.100.101.1</IPAddress>
<port xsi:type="xsd:unsignedInt" >80</port>
< /ns:addlbvserver >
```

The following is the XML response for the above request:

```
<ns:addlbvserverResponse>
<rc xsi:type="xsd:unsignedInt">0</rc>
<message xsi:type="xsd:string">Done</message>
</ns:addlbvserverResponse>
```

B.8 Example: Querying the NetScaler Configuration

This example shows an API request that queries the NetScaler configuration and receives a list of entities.

Note: The actual API method and the XML SOAP message contents may differ from the example shown below.

The following is the CLI command to show the configured Load Balancing virtual servers:

show lb vservers

This is an example of the output of the **show lb vservers** CLI command:

```
>show lb vservers
         2 configured virtual server:
1)  vipLB1 (10.100.101.1:80) - HTTP Type: ADDRESS State:
    DOWN
    Method: LEASTCONNECTION Mode: IP
    Persistence: NONE
2)  vipLB2 (10.100.101.2:80) - HTTP Type: ADDRESS State:
    DOWN
    Method: LEASTCONNECTION Mode: IP
    Persistence: NONE
Done
```

The following is the corresponding API method to show the list of Load Balancing virtual servers:

```
ns__getlbvserver(handle, NULL, &out)
```

The following is the XML request:

```
<ns:getlbvserver></ns:getlbvserver>
```

The following is the XML Response for the above request:

```
<ns:getlbvserverResponse>
  <rc xsi:type="xsd:unsignedInt">0</rc>
  <message xsi:type="xsd:string">Done</message>
  <List xsi:type="SOAP-ENC:Array"
     SOAP-ENC:arrayType="ns:lbvserver[2]">
    <item xsi:type="ns:lbvserver">
      <vServerName xsi:type="xsd:string>vipLB1
      </vServerName>
      <serviceType xsi:type="xsd:string>HTTP</serviceType>
      <IPAddress xsi:type="xsd:string >10.100.101.1
      </IPAddress>
      <port xsi:type="xsd:unsignedInt">80</port>
    </item>
    <item xsi:type="ns:lbvserver">
      <vServerName xsi:type="xsd:string>vipLB2
      </vServerName>
      <serviceType xsi:type="xsd:string>HTTP</serviceType>
      <IPAddress xsi:type="xsd:string >10.100.101.2
      </IPAddress>
      <port xsi:type="xsd:unsignedInt">80</port>
    </item>
  </List>
</ns:getlbvserverResponse>
```

B.9 The Web Service Definition Language (WSDL)

The interface schema provided by NetScaler enables the development of client applications that use the API in a language and platform with which the developer is comfortable. This interface schema is based on the WSDL specification.

NetScaler provides a WSDL file (`NSConfig.wsdl`) containing the interface definition. Developers, with the help of a third-party tool (such as, **gSOAP**) can use this WSDL file to generate client "stubs". These stubs are then called in a custom application to send a request to NetScaler. The application can be in any of the languages supported by the third-party tool. For example, Java, C, or C++.

The `NSConfig.wsdl` file is available on the NetScaler box at:

`http://`<*NSIP*>`/API/NSConfig.wsdl`

where:

NSIP is the IP address of your NetScaler box.

Use this WSDL file and the interfaces mentioned in this document to develop customized applications.

B.10 Creating Client Applications using the NSConfig.wsdl File

A client application can be created by importing the `NSConfig.wsdl` with the **gSOAP** WSDL Importer to create a header file with the C/C++ declarations of the SOAP methods. The **gSOAP** compiler is then used to translate this header file into stubs for the client application.

The following are the steps to create client stubs using the `NSConfig.wsdl` file:

1. Get the NSConfig.h header file from the WSDL file, using the wsdl2h program that comes with gSOAP:

   `./wsdl2h NSConfig.wsdl`

Output

```
**  The gSOAP WSDL parser for C and C++ 1.0.2
**  Copyright (C) 2001-2004 Robert van Engelen, Genivia, Inc.
**  All Rights Reserved. This product is provided "as is", without any warranty.
Saving NSConfig.h
Reading file 'NSConfig.wsdl'
Cannot open file 'typemap.dat'
```

```
Problem reading type map file typemap.dat.
Using internal type definitions for C instead.
```

To complete the process, compile with:

```
soapcpp2 NSConfig.h
```

2. Generate the XML files and stubs:

```
./soapcpp2 -c -i NSConfig.h
```

```
Output:
**  The gSOAP Stub and Skeleton Compiler for C and C++ 2.4.1
**  Copyright (C) 2001-2004 Robert van Engelen, Genivia, Inc.
**  All Rights Reserved. This product is provided "as is", without any warranty.
Saving soapStub.h
Saving soapH.h
Saving soapC.c
Saving soapClient.c
Saving soapServer.c
Saving soapClientLib.c
Saving soapServerLib.c
Using ns1 service name: NSConfigBinding
Using ns1 service location: http://netscaler.com/api
Using ns1 schema namespace: urn:NSConfig Saving
soapNSConfigBindingProxy.h client proxy Saving
soapNSConfigBindingObject.h server object Saving
NSConfigBinding.addserver.req.xml sample SOAP/XML request
Saving NSConfigBinding.addserver.res.xml sample SOAP/XML
response Saving NSConfigBinding.disableserver.req.xml
sample SOAP/XML request Saving
NSConfigBinding.disableserver.res.xml sample SOAP/XML
response Saving NSConfigBinding.enableserver.req.xml
sample SOAP/XML request Saving
NSConfigBinding.enableserver.res.xml sample SOAP/XML
response
    [ ... Similar lines clipped ... ]
```

```
Saving NSConfigBinding.nsmap namespace mapping table
Compilation successful
```

This creates the stub files soapC.c, soapClient.c and stdsoap2.c.

Link them with your source code to create a stand-alone binary that invokes the Netscaler API.

B.11 Securing NetScaler API Access

Secure access to NetScaler CLI objects can be provided based on the NetScaler IP address or on the subnet IP address on which the NetScaler 9000 system is deployed.

B.11.1 Secure NetScaler API Access Based on NetScaler IP

To provide secured API access based on the NetScaler IP address, configure the NetScaler 9000 system to use transparent SSL mode with clear text port using the following configuration steps:

1. Create a loopback SSL service and configure it use transparent SSL mode with clear text port, by entering the following CLI command:

   ```
   add service secure_xmlaccess 127.0.0.1 SSL 443
   -clearTextPort 80
   ```

2. Add certificate and key

   ```
   add certkey cert1 –cert /nsconfig/ssl/ssl/cert1024.pem
   –key /nsconfig/ssl/ssl/rsakey.pem
   ```

   Note: You can use an existing certificate and key or use the “NetScaler Certificate Authority Tool” to create key and test certificate for secure access.

3. Bind the Certificate and the Key to the service using the following CLI command:

   ```
   bind certkey secure_xmlaccess cert1 -Service
   ```

4. Add a custom TCP monitor to monitor the SSL service you have added:

   ```
   add monitor ssl_mon TCP -destport 80
   ```

5. Bind the custom TCP monitor to the SSL service using the following CLI command:

   bind monitor ssl_mon secure_xmlaccess

B.11.2 Secure NetScaler API Access Based on Subnet IP

To secure NetScaler API access based on the subnet IP:

1. Create a SSL VIP and the IP address of this VIP should be in the respective subnet. Use the following command at the CLI prompt:

   add vserver <*vServerName*> **SSL** <*Subnet-IP*> **443**

2. Create a loopback HTTP service by entering the following CLI command:

   add service <*serviceName*> **127.0.0.1 HTTP 80**

3. Bind the service to the SSL VIP using the following command.

   bind lb vserver <*vServerName*> <*serviceName*>

4. Add the certificate and the key using the following CLI command:

   add certkey cert1 –cert /nsconfig/ssl/ssl/cert1024.pem –key /nsconfig/ssl/ssl/rsakey.pem

Note: You can use an existing certificate and key or use the “NetScaler Certificate Authority Tool” to create key and test certificate for secure access.

5. Bind the Certificate and the Key to the SSL VIP using the following CLI command:

   bind certkey <*vServerName*> **cert1**

Appendix C: Warning and Safety Messages

SAFETY PERSONNEL WARNING

WarningThis equipment is to be installed and maintained by authorized and trained service personnel only.

Attention Cet équipement doit être installé et maintenu seulement par du personnel d'entretien.

QUALIFIED PERSONNEL WARNING

WarningOnly trained and qualified personnel should be allowed to install or replace this equipment.

Attention Tout installation ou remplacement de l'équipement doit être fait par du personnel qualifié et compétent.

INSTALLATION WARNING

WarningRead the installation instructions carefully before you connect the system to its power source.

Attention Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

JEWELRY REMOVAL WARNING

WarningBefore getting down to work on equipment that is connected to live power lines, remove jewelry items (including rings, necklaces, and watches). Metal objects canl heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Attention Avant d'accéder à cet équ ipement connecté aux lignes électriques, arracher tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

STACKING THE CHASSIS WARNING

WarningDo not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

Attention Ne placez pas ce châssis sur un autre appareil. En cas de chute, il pourrait provoquer de graves blessures corporelles et équipement dommage.

MAIN DISCONNECTING DEVICE

WarningThe plug-socket combination must be accessible at all times because it serves as the main power disconnecting device.

Attention La combinaison de prise de courant doit être accessible à tout moment parce qu'elle fait office de système principal de déconnexion.

TN POWER WARNING

WarningThe device is designed to work with TN power systems.

Attention Ce dispositif a été conçu pour fonctionner avec des systèmes d'alimentation TN.

GROUND CONNECTION WARNING

WarningWhen installing the unit, the ground connection must always be made first and disconnected last.

Attention Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.

GROUNDED EQUIPMENT WARNING

WarningThe equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Attention Cet équipement doit être relié à la terre. S'assurer que l'appareil hôte est relié à la terre lors de l'utilisation normale.

CIRCUIT BREAKER (15 A) WARNING

WarningThis product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on the phase conductors (all current-carrying conductors).

Attention Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 16 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

NO ON/OFF SWITCH WARNING

WarningUnplug the power cord before you work on a system that does not have a power on/off switch.

Attention Avant de travailler sur un système non équipé d'un commutateur marche-arrêt, débrancher le cordon d'alimentation.

SUPPLY CIRCUIT WARNING

WarningCare must be given while/before connecting units to the supply circuit so that the wiring is not overloaded.

Attention Veillez à bien connecter les unités au circuit d'alimentation afin de ne pas surcharger les connections.

LIGHTNING ACTIVITY WARNING

WarningDo not work on the system or connect or disconnect cables during periods of lightning activity. This product relies on the building's installation for short-circuit (overcurrent).

Attention Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage. Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local.

POWER SUPPLY WARNING

WarningDo not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.

Attention Ne pas toucher le bloc d'alimentation quand le cordon d'alimentation est branché. Avec les systèmes munis d'un commutateur marche-arrêt, des tensions de ligne sont présentes dans l'alimentation quand le cordon est branché, même si le commutateur est à l'arrêt. Avec les systèmes sans commutateur marche-arrêt, l'alimentation est sous tension quand le cordon d'alimentation est branché.

CHASSIS WARNING — RACK MOUNTING AND SERVICING

WarningTo prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

AttentionPour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel:

- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.
- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.
- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

PRODUCT DISPOSAL WARNING

WarningUltimate disposal of this product should be handled according to all national laws and regulations.

Attention La mise su rebut ou te recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environment. Renseignez-vous auprès de l'organisme compétent.

BATTERY HANDLING/REPLACEMENT WARNING

WarningThere is the danger of explosion if the battery (CR 2032) is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Attention Danger d'explosion si la pile (batterie) (CR 2032) n'est pas remplacée correctement. Ne la remplacer que par une pile (batterie) de type équivalent, recommandée par le fabricant. Jeter les piles (batteries) usagées conformément aux instructions du fabricant.

SAFETY LABEL CAUTION

CautionNever remove the cover on a power supply or any part that has the following label attached:

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact NetScaler 9000 system Technical Support.